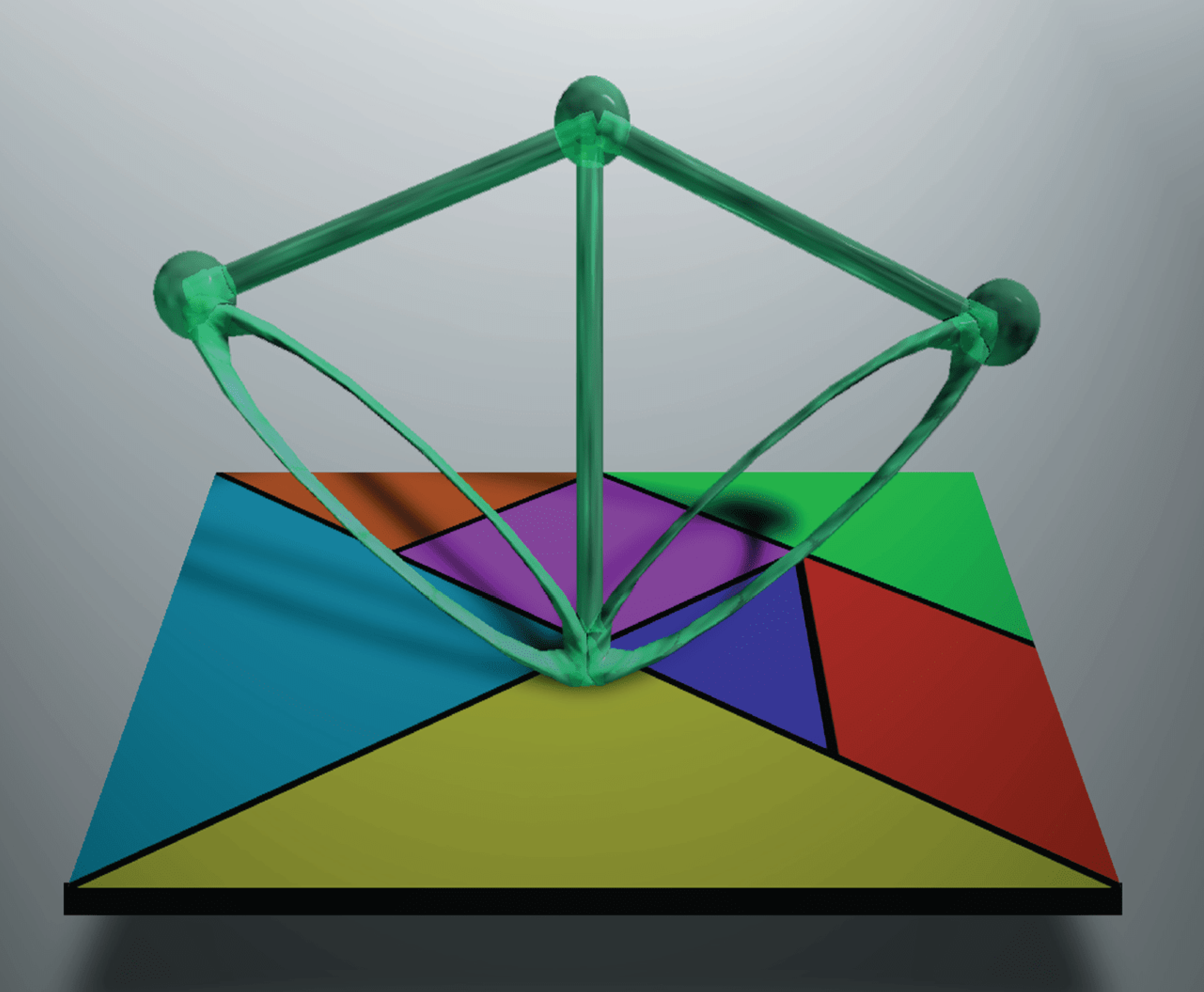
计算机科学组合学丛书

信息安全的数学基础

信息安全的数学基础

卢华明 编著



清华大学出版社

清华大学出版社

计算机科学组合学丛书

信息安全的数学基础

卢华明　编著

清华大学出版社
北　京

内 容 简 介

在信息时代，信息是时间也是财富，这已是不争的事实。所以如何保护信息的安全，已经提到日程上来了。但研究信息安全涉及众多的数学基础，本书的目的也就是为研究信息安全提供必要的数学内容，主要内容包括数论、群论、组合论、素数的判定法、椭圆曲线、信息论等。

图书在版编目(CIP)数据

信息安全的数学基础/卢华明编著. —北京：清华大学出版社，2016
(计算机科学组合学丛书)
ISBN 978-7-302-38316-1

Ⅰ. ①信…　Ⅱ. ①卢…　Ⅲ. ①信息安全—应用数学　Ⅳ. ①TP309 ②O29

中国版本图书馆 CIP 数据核字(2014)第 242054 号

责任编辑：张　民　薛　阳
封面设计：傅瑞学
责任校对：李建庄
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：三河市少明印务有限公司
开　　本：185mm×260mm　　**印　　张**：11.25　　**字　　数**：279 千字
版　　次：2016 年 4 月第 1 版　　**印　　次**：2016 年 4 月第1 次印刷
印　　数：1～2000
定　　价：29.90 元

产品编号：042349-01

前　言

在信息时代，信息是时间也是财富，信息的安全还关系到国家的安全。保护信息的安全不仅是军队和政府部门的需要，更是民间企业和银行金融系统的需要，这已经是不争的事实。信息安全的支柱是密码和编码，它们从政府和军营走出，走入平民百姓家，反过来又极大地促进了密码、编码的发展。总而言之，从事信息科学首先必须了解它的安全性问题是回避不了的。

密码和编码需要近代数学的支持，本书的目的就是为此做准备。编者在北京信息科技大学执教数学多年，更深切地感到其急迫性，故愿抛砖引玉。但密码和编码用到的数学知识非常多，本书仅涉及最主要的方面，就这样挂一漏万也在所难免，望读者见谅！

全书适合作为相关专业研究生的读物，前 4 章也可作为本科生的教材。

编　者

2016 年 3 月

符 号 约 定

$\mathbf{N}=\{1,2,3,\cdots\}$

$\mathbf{N}^*=\{0,1,2,\cdots\}$

$\mathbf{Z}=\{\cdots,-2,-1,0,1,2,\cdots\}$

$\mathbf{R}$=实数集，$\mathbf{R}^+$=正实数

$\mathbf{Q}$=有理数集

$\lfloor x \rfloor$：表示比 x 数小的最大整数

$\lceil x \rceil$：表示比 x 数大的最小整数

$a|b$：表示数 a 除尽数 b

$a\nmid b$：表示数 a 不能除尽数 b

(a,b)：即 $\gcd(a,b)$，即数 a 和数 b 的最大公约数

$[a,b]$：即 $\mathrm{lcm}(a,b)$，即数 a 和数 b 的最小公倍数

$O(n^k)$：比如 $f\equiv O(n^k)$ 表示存在常数 C 使 $f<C_n^k$

$\prod$：表示连乘积，如 $\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \cdots \cdot a_n$

$\sum$：表示求和，如 $\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$

令 $O(f)=\{g:N\to R^+ \mid \exists c\in R^+, \exists n_0\in N, \forall n\geqslant n_0, g(n)=cf(n)\}$

令 $\Omega(f)=\{g:N\to R \mid \exists n_0\in N, \exists c\in R^+, \forall n\geqslant n_0, cf(n)<g(n)\}$

$\Theta(f)=O(f)\cap\Omega(f)$

$\forall$：所有，如 $\forall n\geqslant n_0$ 指大于或等于 n_0 的所有数 n

$\to$：映射，如 $N\to R$ 指由正整数到实数的映射，或由 N 到 R 的函数

目　　录

第 1 章　数　　论

1.1　整　　数

整数通常都采用十进制表示，比如 5 876 943，即

$$5\times 10^6+8\times 10^5+7\times 10^4+6\times 10^3+9\times 10^2+4\times 10+3$$

但在电子计算机中，数的十进制表示就很不方便了，而是采用以 2 为基来表示数。其实任一正整数 b 都可以用来作基。任何整数 n 都可以唯一地表示为

$$n=a_h\times b^h+a_{h-1}\times b^{h-1}+\cdots+a_1\times b+a_0$$

或表示为 $(a_na_{n-1}\cdots a_1a_0)_b$，$a_n$、$a_{n-1}$、$\cdots$、$a_1$、$a_0$ 可依次通过 n 除以 b 求得。n 除以 b 可得商 q_0 及余数 a_0。即

$$n=q_0b+a_0,\quad 0\leqslant a_0\leqslant b-1$$

若 $q_0\neq 0$，则继续除以 b，得

$$q_0=q_1b+a_1\quad 0\leqslant a_1\leqslant b-1$$

继续以上的过程，

$$\begin{aligned}
q_1&=q_2b+a_2\quad 0\leqslant a_2\leqslant b-1\\
q_2&=q_3b+a_3\quad 0\leqslant a_3\leqslant b-1\\
&\vdots\\
q_{h-2}&=q_{h-1}b+a_{h-1}\quad 0\leqslant a_{h-1}\leqslant b-1\\
q_{h-1}&=a_h\quad 0\leqslant a_h\leqslant b-1
\end{aligned}$$

最后一步到商为零。

$$\begin{aligned}
n&=q_0b+a_0=(q_1b+a_1)b+a_0=q_1b^2+a_1b+a_0\\
&=(q_2b+a_2)b^2+a_1b+a_0=q_2b^3+a_2b^2+a_1b+a_0\\
&=\cdots=(q_{h-1}b+a_{h-1})b^{h-1}+a_{h-2}b^{h-1}+\cdots+a_1b+a_0\\
&=a_hb^h+a_{h-1}b^{h-1}+\cdots+a_1b+a_0
\end{aligned}$$

所以

$$n=a_hb^h+a_{h-1}b^{h-1}+\cdots+a_1b+a_0=(a_ha_{h-1}\cdots a_1a_0)_b$$

而且这种表示法是唯一的，否则若

$$n=c_hb^h+c_{h-1}b^{h-1}+\cdots+c_1b+a_0$$

将出现

$$n=(c_h-a_h)b^h+(c_{h-1}-a_{h-1})b^{h-1}+\cdots+(c_1-a_1)b+(c_0-a_0)$$

n 展成以 b 为基的表达式，故

$$c_h=a_h、c_{h-1}=a_{h-1}、\cdots、c_0=a_0$$

例 1-1　试将 1865 用二进制表示。

解： 1865＝2×932＋1

$932=2\times466+0$

$466=2\times233+0$

$233=2\times116+1$

$116=2\times58+0$

$58=2\times29+0$

$29=2\times14+1$

$14=2\times7+0$

$7=2\times3+1$

$3=2\times1+1$

$1=2\times0+1$

所以

$$1865=(1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1)_2$$

例 1-2 $b=16$，用 A 表示 10、B 表示 11、C 表示 12、D 表示 13、E 表示 14、F 表示 15，求$(A\quad 3\quad 5\quad B\quad 0\quad F)_{16}$的十进制表示。

解：
$$\begin{aligned}(A\quad 3\quad 5\quad B\quad 0\quad F)_{16}&=10\times16^5+3\times16^4+5\times16^3+11\times16^2+15\\&=10\ 485\ 760+196\ 608+20\ 480+2816+15\\&=(1\ 0\ 7\ 0\ 5\ 6\ 7\ 9)_{10}\end{aligned}$$

例 1-3 试求$(A\quad 3\quad 5\quad B\quad 0\quad F)_{16}$的二进制表示。

解：当然可以从$(A\quad 3\quad 5\quad B\quad 0\quad F)_{16}$的十进制表示$(1\ 0\ 7\ 0\ 5\ 6\ 7\ 9)_{10}$再二进制化。但十六进制和二进制也有直接关系，如表 1-1 所示。

表 1-1 二进制与十六进制的关系

十六进制	二进制表示	十六进制	二进制表示	十六进制	二进制表示	十六进制	二进制表示
0	0000	4	0100	8	1000	C	1100
1	0001	5	0101	9	1001	D	1101
2	0010	6	0110	A	1010	E	1110
3	0011	7	0111	B	1011	F	1111

所以

$$(A\quad 3\quad 5\quad B\quad 0\quad F)_{16}=(1\ 0\ 1\ 0\quad 0\ 0\ 1\ 1\quad 0\ 1\ 0\ 1\quad 1\ 0\ 1\ 1\quad 0\ 0\ 0\ 0\quad 1\ 1\ 1\ 1)_2$$

例 1-4 将$(1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1)_2$化成十六进制数。

解：
$$\begin{aligned}(1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1)_2&=(0\ 0\ 1\ 1\quad 1\ 1\ 0\ 1\quad 1\ 1\ 1\ 0\quad 1\ 0\ 0\ 1)_2\\&=(3\ D\ E\ 9)_{16}\end{aligned}$$

1.2 素 数

一个大于 1 且只能被 1 及它自身除尽的正整数，称为素数。

如 2、3、5、7、11 便是素数。不是素数的数称为合数，而且每一个大于 1 的正整数必有素数因子。

定理 1-1：素数是无穷多的。

证 如若不然，假设有最大的素数 p，令 $n=2\times3\times5\times\cdots\times p+1$。

n 是大于 1 的正整数，不能被已知所有的素数除尽，所以 n 本身也是素数，与 p 是最大素数的假定矛盾。所以素数的数目是无穷多的。

定理 1-2：若 n 是合数，则 n 有不超过$\sqrt{n}$的素数因数。

证 因 n 是合数，令 $n=a\cdot b$，$1\leqslant a\leqslant b\leqslant n$，必有 $a\leqslant\sqrt{n}$，若$\sqrt{n}<a\leqslant b$，则 $ab>\sqrt{n}\cdot\sqrt{n}=n$ 和 $n=a\cdot b$ 的假定矛盾，所以 n 有不超过$\sqrt{n}$的素数因数。

利用以上定理可以找出所有小于正整数 n 的所有素数。其方法是由希腊数学家 Erarosthenenes 提出的。

例 1-5 以 $n=100$ 为例，找出小于 100 的全部素数。

解：在 1～100 的数列中依次对 2，3，5，7 的倍数引入 /、\、—、| 的标志。

如表 1-2 所示，没划线的数都是素数：2、3、5、7、11、13、17、19、23、29、31、37、41、43、47、53、59、61、67、71、73、79、83、89、97，共 25 个素数。

表 1-2 判定素数 Erarosthenenes 法

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

这种判定素数的方法无疑效率极为低下。关于素数问题的研究一直延续到今天，始终没有间断。

令 $\pi(x)$表示比 x 小的素数的数目，则有 $\pi(x)\sim\frac{x}{\ln x}$，证明从略。

1.3 最大公约数与欧几里得算法

定义 1-1：非零的两个整数 a 和 b，除尽 a 和 b 的最大整数称为 a 和 b 的最大公约数，记为(a,b)或 $\gcd(a,b)$。被 a 和 b 除尽的最小整数，称为 a 和 b 的最小公倍数，记为$[a,b]$或 $\text{lcm}(a,b)$。

定理 1-3：每一个整数 n，可唯一地将它分解为 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，其中 $p_1,p_2,\cdots,p_k$ 是

两两互异的素数，而且 α_1、α_2、…、α_k 是正整数。

证 用数学归纳法证明。

当 $n=2$ 时上结论正确。

当 $n>2$ 时，假定在 $1\sim n$ 之间的每一个正整数都可以唯一地分解成素数次方的乘积。

若 n 是素数，则 $n=n\times1$，如若不然，n 是合数，即 $n=a\cdot b$，$1<a\cdot b<n$，a 和 b 都可以分解成素数次方的乘积，以之代入 $n=a\cdot b$，即得一组素数的次方的乘积。

下面证 n 分解为 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 是唯一的。

用反证法，假定 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=q_1^{\beta_1}q_2^{\beta_2}\cdots q_k^{\beta_k}$，其中 p_1、p_2、…、p_k 和 q_1、q_2、…，q_k是两两不同的素数，α_i和 β_i都是正整数，$i=1,2,\cdots,k$。

对于 $n=q_1^{\beta_1}q_2^{\beta_2}\cdots q_k^{\beta_k}$，由于 $p_1|n$，所以不失一般性，假定 $p_1|q_1$。

n 除以 p_1 得 $p_1^{\alpha_1-1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=q_1^{\beta_1-1}q_2^{\beta_2}\cdots q_h^{\beta_h}$。

反复利用以上步骤，最后等式一端被其素数因数除尽，结果为 1。而另一端成为 p_i 的素数次方之积，或为 q_i 的素数次方之积。这是不可能的。所以只能 $p_i=q_i$、$\alpha_i=\beta_i$，$i=1,2,\cdots,k$，$h=k$。

假定

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\quad b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$$

则

$$ab=p_1^{\alpha+\beta_1}p_2^{\alpha_2+\beta_2}\cdots p_k^{\alpha_k+\beta_k}$$
$$a/b=p_1^{\alpha-\beta_1}p_2^{\alpha_2-\beta_2}\cdots p_k^{\alpha_k-\beta_k}$$
$$\gcd(a,b)=p_1^{\min(\alpha,\beta_1)}p_2^{\min(\alpha_2,\beta_2)}\cdots p_k^{\min(\alpha_k,\beta_k)}$$
$$\mathrm{lcm}(a,b)=p_1^{\max(\alpha,\beta_1)}p_2^{\max(\alpha_2,\beta_2)}\cdots p_k^{\max(\alpha_k,\beta_k)}$$

定义 1-2：两整数 a 和 b，若 $(a,b)=1$，则称 a 与 b 互素。

定理 1-4：设 $(a,b)=d$，则① $\left(\frac{a}{d},\frac{b}{d}\right)=1$；② $(a+cb,b)=(a,b)$。

证 （1）若存在整数 e，则 $e\left|\frac{a}{d}\right.$，设 $\frac{a}{d}=he$，$a=bed$，$e\left|\frac{b}{d}\right.$，$\frac{b}{d}=ke$，$b=ked$，但 $(a,b)=d$，即 $(a,b)=ed=d$，所以 $e=1$。

（2）假定 $d=(a,b)$，则 $d|(a+cb)$，即 d 是 $a+c$ 和 b 的公因数。d 是 $a+bc$ 和 b 的公因数，则 $d=(a+cb-cb,b)$。即

$$d=(a,b),\quad (a+cb,b)=(a,b)$$

下面介绍求 $\gcd(a,b)$ 的欧几里得算法。

引理：已知整数 a 和 b，且 $a>b$、$a=qb+r$、$0<r<b$，则 $(a,b)=(b,r)$。

证 由于 $a=qb+r$，若 $c|a$、$c|b$，则 $c|r$，所以 a 和 b 的最大公约数也是 b 和 r 的最大公因数，即 $(a,b)=(b,r)$。

欧几里得算法：若令 $r_0=a$、$r_1=b$，令 $r_j=q_{j+1}r_{j+1}+r_{j+2}$，$0\leqslant r_{j+2}<r_{j+1}(j=1,2,\cdots,n-2)$。使 $r_{n+1}=0$，则 $r_{n+1}=(a,b)$。

下面先举一例，叙述欧几里得算法，然后再证明其正确性。

例 1-6　求(252,198)。

解：252＝1×198＋54　54＝252－198

198＝3×54＋36　36＝198－3×54

54＝1×36＋18　18＝54－36

36＝2×18　(252,198)＝18

(252,198)＝(198,54)＝(54,36)＝(36,18)＝18

证　$r_0=a, r_1=b, a\geqslant b$,连续利用除法得

$$r_0 = q_1 r_1 + r_2 \quad 0 \leqslant r_2 < r_1$$
$$r_1 = q_2 r_2 + r_3 \quad 0 \leqslant r_3 < r_2$$
$$\vdots$$
$$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad 0 \leqslant r_n < r_{n-1}$$
$$r_{n-1} = q_n r_n \quad r_{n+1} = 0$$
$$(a,b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n$$

所以$(a,b)=r_n$

而且可以证明存在整数 l 和 m，使$(a,b)=la+mb$。

以(252,198)＝18 为例：

$$18 = 54 - 36 = 54 - (198 - 3\times 54) = 4\times 54 - 198$$
$$= 4\times(252 - 198) - 198 = 4\times 252 - 5\times 198$$

1.4　欧几里得算法复杂性讨论

算法复杂性研究是计算机科学的一门重要课题，所谓算法的复杂性，也就是对解决问题的过程中计算量的估计。一般来说，计算量越小的算法越好。但对于设计密码学来说恰恰相反，计算量越大，破译的难度越高，密码的抗攻击能力就越强。从算法复杂性研究密码学，开阔了一个“引人入胜”的领域。

讨论欧几里得算法的复杂性还需要做些准备，首先是对 Fibonacci 序列的估计式的讨论。递推关系 $F_n=F_{n-1}+F_{n-2}$、$F_1=F_2=1$，于是得序列：$F_1=F_2=1$、$F_3=F_2+F_1=2$、$F_4=F_3+F_2=3$……即可得 Fibonacci 序列为：1、1、2、3、5、8、13、21……

估计式：

$$F_n > \left[\frac{1}{2}(1+\sqrt{5})\right]^{n-2}$$

求证：

$$F_3 = 2 > \left[\frac{1}{2}(1+\sqrt{5})\right]^{3-2} = \frac{1}{2}(1+\sqrt{5})$$

证　假定不等式 n 时成立，即 $F_n > \left[\frac{1}{2}(1+\sqrt{5})\right]^{n-2}$ 成立，下证 $n+1$ 时，$F_{n+1} > \left[\frac{1}{2}(1+\sqrt{5})\right]^{n-1}$ 成立。

$x=\frac{1}{2}(1+\sqrt{5})$满足 $x^2-x-1=0$，令 $\alpha=\frac{1}{2}(1+\sqrt{5})$，则有 $\alpha^2=\alpha+1$。根据假定有：

$$\alpha^{n-1} = \alpha^2 \cdot \alpha^{n-3} = (1+\alpha) \cdot \alpha^{n-3} = \alpha^{n-3} + \alpha^{n-2} < F_{n-1} + F_n = F_{n+1}$$

即

$$F_{n+1} > \alpha^{n-1} = \left[\frac{1}{2}(1+\sqrt{5})\right]^{n-1}$$

证毕

欧几里得算法的计算量在于估计作除法运算的数量，结论是：除法次数不超过 a、b 两数中小的一个数的 10 进位数的 5 倍。

证 $r_0 = a,\quad r_1 = b$

$$F_{n+1} > \left[\frac{1}{2}(1+\sqrt{5})\right]^{n-1}$$

$$r_0 = q_1 r_1 + r_2 \quad 0 \leqslant r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \quad 0 \leqslant r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad 0 \leqslant r_n < r_{n-1}$$

$$r_{n-1} = q_n r_n$$

共作 n 次除法，其中 q_1、q_2、…、q_{n-1} 都是大于 1 或者等于 1 的整数。$q_n \geqslant 2$、$r_n < r_{n-1}$。于是

$$r_1 \geqslant 1 = F_2 \quad r_{n-1} > 2r_n > 2F_n = F_3$$

$$r_{n-2} \geqslant r_{n-1} + r_n \geqslant F_3 + F_2 = F_4$$

$$r_{n-3} \geqslant r_{n-2} + r_{n-1} \geqslant F_4 + F_3 = F_5$$

$$\vdots$$

$$r_2 \geqslant r_3 + r_4 \geqslant F_{n-1} + F_{n-2} = F_n$$

$$b = r_1 \geqslant r_2 + r_3 \geqslant F_n + F_{n+1} > \left[\frac{1}{2}(1+\sqrt{5})\right]^{n-1}$$

$$\log_{10} b > (n-1)\log_{10}\left[\frac{1}{2}(1+\sqrt{5})\right] = 0.208\,998\,76 \times (n-1) > (n-1)/5$$

$$(n-1) < 5\log_{10} b$$

假定 b 是 k 位十进制数，$b < 10^k$、$\log_{10} b < k$，$(n-1) < 5k$、$n \leqslant 5k$。

证毕

1.5 大数的因数分解

前面已经介绍，比 N 小的素数的数目为 $\pi(N) \sim \dfrac{N}{\ln N}$，～表示近似的意思。

若 $N = 10^{10}$，$\dfrac{N}{\ln N} = \dfrac{10^{10}}{23.026} = 4.343 \times 10^8$。

也就是说，小于 10^{10} 的素数数目接近 4.343×10^8。

对于数 10^{20}，要对它进行因数分解，它的因数不超过 $\sqrt{10^{20}} = 10^{10}$。要对它进行因数分解，在最坏的情况下要对 4.343×10^8 个素数进行除法运算。假定已有大到 10 位的十

进制素数表，用每秒对十进制数 50 位的数作每秒 100 万次除法运算，需用时：

$$T = \frac{4.343 \times 10^8}{10^6} = 4.343 \times 10^2 = 434.3(\mathrm{s}) = \frac{434.3}{3600}(\mathrm{h}) = 0.121(\mathrm{h})$$

例 1-7　$N=5\times10^{50}$，即对 50 位的十进制数进行因数分解，小于 $\sqrt{N}$ 的素数数目有：

$$\frac{\sqrt{5\times10^{50}}}{\ln\sqrt{5\times10^{50}}} = \frac{2.236\times10^{25}}{58.369} = 3.8308\times10^{23}$$

根据上题的最坏情况，考虑要做 3.8308×10^{23} 次十进制数 50 位数的除法。用每秒做十进制数 50 位的数作 100 万次除法的快速电子计算机进行运算，需用时：

$$T = \frac{3.8308\times10^{23}}{10^6} = 3.8308\times10^{17} = \frac{3.8308\times10^{17}}{365\times24\times3600} = \frac{3.8308\times10^{17}}{3.1536\times10^7}$$
$$=1.2148\times10^{10}(\text{年})$$

这说明当 N 增加到 5×10^{50} 时，最坏情况下需要每秒进行 50 位十进制数除法 100 万次的计算机运行时间超过 10^{10} 年。10^{10} 年是什么概念呢？它是亿万年。

这里还不包括对 3.8308×10^{23} 个素数如何判定，大数的分解是密码学的重要问题，也是一个难题，这里先提供一些直观的概念。

1.6　同　余　式

定义 1-3：令 m 是一正整数，a 和 b 是整数，若 $m|(a-b)$，则称 mod m，a 和 b 同余，用 $a\equiv b(\bmod m)$ 来表示。若 $m\nmid(a-b)$ 则称 mod m，a 和 b 不同余，用 $a\not\equiv b(\bmod m)$ 来表示。

例如：$24\equiv2(\bmod 11)$，因 $11|(24-2)$。故 $24-2$ 和 $12-1$ mod n 同余，n 是任一整数。

定理 1-5：a 和 b 是整数，$a\equiv b(\bmod m)$ 的充要条件是存在整数 l，使得 $a=b+lm$。

证　因 $a\equiv b(\bmod m)$，则 $m|(a-b)$，即存在整数 l，使 $a=b+lm$。

反过来，若 $a=b+lm$，则 $a-b=lm$、$m|(a-b)$，所以 $a\equiv b(\bmod m)$。

定理 1-6：(1) 若 a 是整数，则 $a\equiv a(\bmod m)$。

(2) 若 a 和 b 是整数，而 $a\equiv b(\bmod m)$，则 $b\equiv a(\bmod m)$。

(3) 若 a、b、c 是整数，且 $a\equiv b(\bmod m)$、$b\equiv c(\bmod m)$，则 $a\equiv c(\bmod m)$。

证　(1) 因 $m|(a-a)$，即 $m|0$，故 $a\equiv a(\bmod m)$。

(2) 因 $a\equiv b(\bmod m)$，则 $a=b+lm$，l 是整数。$b-a=(-l)m$，所以 $b\equiv a(\bmod m)$。

(3) $a\equiv b(\bmod m)$，则 $a=b+hm$。又因 $b\equiv c(\bmod m)$，则 $b=c+km$。h 和 k 都是整数，所以 $a=c+(h+k)m$，即 $a\equiv c(\bmod m)$。

mod m 表示将整数分成 m 个同余类。以 $m=5$ 为例：

$$\{\cdots,-10,-5,0,5,10,\cdots\}: a\equiv0(\bmod 5)$$
$$\{\cdots,-9,-4,1,6,11,\cdots\}: a\equiv1(\bmod 5)$$
$$\{\cdots,-8,-3,2,7,12,\cdots\}: a\equiv2(\bmod 5)$$
$$\{\cdots,-7,-2,3,8,13,\cdots\}: a\equiv3(\bmod 5)$$

$$\{\cdots,-6,-1,4,9,14,\cdots\}: a\equiv 4 \pmod 5$$

定理 1-7：a、b、c 是整数，m 是正整数，而且 $a\equiv b\pmod m$，则①$a+c\equiv b+c\pmod m$；②$a-c\equiv b-c\pmod m$；③$ac\equiv bc\pmod m$。

证 ① 因 $a\equiv b\pmod m$，故 $m|(a-b)$、$(a+c)-(b-c)=a-b$，所以 $m|((a+c)-(b-c))$，所以 $a+c\equiv b+c\pmod m$。

② 类似证 $m|((a-c)-(b-c))$，所以 $a-c\equiv b-c\pmod m$。

③ 因 $m|(a-b)$，所以 $m|c(a-b)$，即 $ac\equiv bc\pmod m$。

定理 1-8：a、b、c、m 是整数，而且 $m>0$、$d=(c,m)$、$ac\equiv bc\pmod m$，则 $a\equiv b\left(\bmod \dfrac{m}{d}\right)$。

证 $ac\equiv bc\pmod m$，所以 $m|(ac-bc)$、$m|c(a-b)$，故存在整数 k 使 $c(a-b)=km$，$d=(c,m)$，用 d 除等式两端得$\dfrac{c(a-b)}{d}=\dfrac{km}{d}$。

由于 $d=(c,m)$，故$\left(\dfrac{c}{d},\dfrac{m}{d}\right)=1$，故$\dfrac{m}{d}|(a-b)$即 $a\equiv b\left(\bmod \dfrac{m}{d}\right)$。

例 1-8 $50\equiv 20\pmod{15}$，$(10,15)=5$，故 $5\equiv 2\pmod 3$。

推论：$ac\equiv bc\pmod m$、$(c,m)=1$，则 $a\equiv b\pmod m$。

定理 1-9：若 a、b、c、d、m 是整数，且 $m>0$，$a\equiv b\pmod m$，$c\equiv d\pmod m$，则①$a+c\equiv b+d\pmod m$；② $a-c\equiv b-d\pmod m$；③$ac\equiv bd\pmod m$。

证 因 $a\equiv b\pmod m$、$c\equiv d\pmod m$，故 $m|(a-b)$、$m|(c-d)$，存在整数 h 和 k，使得 $a-b=hm$、$c-d=km$。

① $(a+c)-(b-d)=(a-b)+(c-d)=(h+k)m$，故 $a+c\equiv b+d\pmod m$。

② $(a-c)-(b-d)=(a-b)-(c-d)=(h-k)m$，故 $a-c\equiv b-d\pmod m$。

③ $ac-bd=ac-bc+bc-cd=(a-b)c-(c-d)b=chm+bkm=(ch+bk)m$，故 $ac\equiv bd\pmod m$。

定理 1-10：a、b、k、m 都是整数，而且 $k>0$、$m>0$、$a\equiv b\pmod m$，则 $a^k\equiv b^k\pmod m$。

证 因 $a\equiv b\pmod m$，故 $m|(a-b)$，$a^k-b^k=(a-b)(a^{k-1}+a^{k-2}b+\cdots+ab^{k-2}+b^{k-1})$，所以 $m|(a^k-b^k)$，即 $a^k\equiv b^k\pmod m$。

例 1-9 求解同余方程 $4x\equiv 11\pmod{13}$。

问题归结为求 $4^{-1}\pmod{13}$，即求 $4y\equiv 1\pmod{13}$。不难得知 $y=(-3)$，$4(-3)=-12\equiv 1\pmod{13}$。用$(-3)$乘 $4x\equiv 11\pmod{13}$ 同余方程两端得

$$x\equiv(-3)\times 11\pmod{13}$$

$x\equiv -33\pmod{13}$即 $x\equiv 6\pmod{13}$。

例 1-10 $a=(a_m a_{m-1}\cdots a_1 a_0)_{10}$、$b=(b_n b_{n-1}\cdots b_1 b_0)_{10}$，若 $ab=(c_l c_{l-1}\cdots c_1 c_0)_{10}$，试证：

$$\left(\sum_{h=0}^{m} a_h \pmod 9\right)\left(\sum_{k=0}^{n} b_k \pmod 9\right)\equiv\sum_{j=0}^{l} c_j \pmod 9$$

$10\equiv 1\pmod 9$、$10^2\equiv 1\pmod 9$、…、$10^m\equiv 1\pmod 9$，所以

$$(a_m a_{m-1}\cdots a_1 a_0)_{10}=a_m\cdot 10^m+a_{m-1}\cdot 10^{m-1}+\cdots+a_1\cdot 10+a_0$$

$$\equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9$$

同理：

$(b_n \cdot 10^n + b_{n-1} \cdot 10^{n-1} + \cdots + b_1 \cdot 10 + b_0) \equiv b_n + b_{n-1} + \cdots + b_1 + b_0 \pmod 9$

$a \cdot b = c = c_l \cdot 10^l + c_{l-1} \cdot 10^{l-1} + \cdots + c_1 \cdot 10 + c_0 \equiv c_l + c_{l-1} + \cdots + c_1 + c_0 \pmod 9$

所以

$$\left(\sum_{i=0}^{m} a_i \pmod 9\right) \cdot \left(\sum_{j=0}^{n} b_j \pmod 9\right) \equiv \sum_{k=0}^{l} c_k \pmod 9$$

这个结果可用来验证乘法的正确性，如果等式成立，乘法不出错的概率比较高，虽然乘法过程会出错，而错到使等式保持相等的概率是非常低的，一般就以等式成立作为判断的准则。

例 1-11　利用 564×353，验证上述结果的正确性。

$$\begin{array}{r} 564 \\ \times\ 353 \\ \hline 1692 \\ 2820 \\ +\ 1692 \\ \hline 199092 \end{array}$$

$$5+6+4 = 1+5 \equiv 6 \pmod 9$$
$$3+5+3 = 6+5 = 11 \equiv 2 \pmod 9$$
$$1+9+9+0+9+2 \equiv 3 \pmod 9$$
$$6 \times 2 = 12 \equiv 3 \pmod 9$$

等式成立，乘法不出错。

若乘法出错而等式成立，则至少一位差了 9，这种错误，达到 9 的机率是很小的。

定理 1-11：若 $a \equiv b \pmod{m_i}$，$(i=1,2,\cdots,k)$，其中 a、b、m_1、m_2、…、m_k 都是整数，而且 m_1、m_2、…、m_k 都是大于 0 的整数，则 $a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$。

证　根据假定 $m_i \mid (a-b)(i=1,2,\cdots,m_k)$，故 $(m_1, m_2, \cdots, m_k) \mid (a-b)$。所以 $a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$，若 m_i是两两互素的整数，则 $a \equiv b \pmod{m_1, m_2, \cdots, m_k}$。

定理 1-12：若$(a,n)=1$，则 $ax \equiv b \pmod m$有一个解，其中 a、b、m 都是整数，而且 $m>0$。

证　因$(a,n)=1$，故 $0a, a, 2a, \cdots, (n-1)a$ 是 mod m 的完全剩余系，必存在整数 h，k，使 $1=ha+kn$，即 $ha \equiv 1 \pmod n$。

用 h 乘同余方程 $ax \equiv b \pmod n$，得

$$hax \equiv hb \pmod n \quad ha \equiv 1 \pmod n$$

故得 $x \equiv hb \pmod n$。

定理 1-13：$(a,n)=d>1$、$d \nmid b$，则 $ax \equiv b \pmod n$ 没有解。

证　若有解 x 使 $ax \equiv b \pmod n$，$d \mid a$，$d \mid n$，于是有 $0x \equiv b \pmod n$，这与 $d \nmid b$ 的假定相矛盾。

所以 $ax \equiv b \pmod n$，$(a,n)=d$，$d \nmid b$ 时无解。

定理 1-14：若$(a,n)=d>1$、$d|b$，则 $ax\equiv b(\mathrm{mod}\ n)$有 d 个解。

证 设 $a=da_1$、$b=ab_1$、$n=dn_1$，于是有 $da_1x\equiv db_1(\mathrm{mod}\ dn_1)$，即 $a_1x\equiv b_1(\mathrm{mod}\ n_1)$、$(a_1,n_1)=1$，故 $a_1x\equiv b_1(\mathrm{mod}\ n_1)$有解。令 $x=\xi$、$x=\xi(\mathrm{mod}\ n_1)$、$0\leqslant\xi<n_1-1$，则 $a_1x\equiv b_1(\mathrm{mod}\ n)$有 d 个解：ξ、$\xi+n_1$、$\xi+2n_1$、…、$\xi+(d-1)n_1$。

1.7 中国剩余定理

早在公元前后，中国的“孙子算经”有记载“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？答曰二十三”，当然后面还给出算法，用现在的方式表达即能联立同余方程组：

$$\begin{cases}x\equiv 2(\mathrm{mod}\ 3)\\x\equiv 3(\mathrm{mod}\ 5)\\x\equiv 2(\mathrm{mod}\ 7)\end{cases}$$

求 x。

所以将求解同余方程组：

$$\begin{cases}x\equiv a_1(\mathrm{mod}\ m_1)\\x\equiv a_2(\mathrm{mod}\ m_2)\\\quad\vdots\\x\equiv a_k(\mathrm{mod}\ m_k)\end{cases}$$

其中，m_1、m_2、…、m_k 两两互素，求解的方法便称为中国剩余定理。下面证 mod $m_1m_2\cdots m_k$，上式有唯一解，证明的过程也就是给出解的过程。

令 $M=m_1m_2\cdots m_k$、$M_j=\dfrac{M}{m_j}(j=1,2,\cdots,k)$，$M_jy_j\equiv1(\mathrm{mod}\ m_j)(j=1,2,\cdots,k)$。

因$(M_j,m_j)=1$，所以存在 M_j^{-1}，使 $M_j^{-1}M_j=1(\mathrm{mod}\ m_j)$。因$(M_j,m_j)=1$，所以存在 h 和 k 两个整数，使 $hM_j+km_j=1$、$hM_j\equiv1(\mathrm{mod}\ m_j)$，$h$ 就是 $M_j^{-1}(\mathrm{mod}\ m_j)$。所以 $y_j\equiv M_j^{-1}(\mathrm{mod}\ m_j)(j=1,2,\cdots,k)$。

令

$$x=M_1y_1a_1+M_2y_2a_2+\cdots+M_ky_ka_k$$

不难验证 $x\equiv a_i(\mathrm{mod}\ m_i)(i=1,2,\cdots,k)$。

请注意所有的 M_j，除 $j-i$ 外都含有 m_i 的因数，所以 $M_iy_ia_i\equiv0(\mathrm{mod}\ m_i)$，$M_iy_ia_i\equiv a_i(\mathrm{mod}\ m_i)$。

例 1-12 求解下式。

$$\begin{cases}x\equiv 2(\mathrm{mod}\ 3)\\x\equiv 3(\mathrm{mod}\ 5)\\x\equiv 2(\mathrm{mod}\ 7)\end{cases}$$

解：$35y_1\equiv1(\mathrm{mod}\ 3)$ $21y_2\equiv1(\mathrm{mod}\ 5)$ $15y_3\equiv1(\mathrm{mod}\ 7)$ $M=3\cdot5\cdot7=105$，

$$M_1=\frac{105}{3}=35, M_2=\frac{105}{5}=21, M_3=\frac{105}{7}=15$$

$35y_1 \equiv 1 (\bmod 3)$　$y_1 \equiv 35^{-1} (\bmod 3)$

$35 = 3 \times 11 + 2$　$3 = 2 + 1$

$1 = 3 - 2 = 3 - (35 - 11 \times 3) = 12 \times 3 - 35$

所以：

$$y_1 \equiv 35^{-1} (\bmod 3) \equiv -1 \equiv 2$$

$$21y_2 \equiv 1 (\bmod 5) \quad y_2 \equiv 21^{-1} (\bmod 5)$$

$$21 = 4 \times 5 + 1 \quad 1 = 21 - 4 \times 5 \quad y_2 \equiv 21^{-1} (\bmod 5) \equiv 1$$

$$15y_3 \equiv 1 (\bmod 7) \quad y_3 \equiv 15^{-1} (\bmod 7)$$

$$15 = 2 \times 7 + 1 \quad 1 = 15 - 2 \times 7 \quad y_3 \equiv 15^{-1} (\bmod 7) \equiv 1$$

$$x = 35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 = 233 \equiv 23 (\bmod 105)$$

例 1-13　求解下式。

$$\begin{cases} x \equiv 1 (\bmod 5) \\ x \equiv 5 (\bmod 6) \\ x \equiv 4 (\bmod 7) \\ x \equiv 10 (\bmod 11) \end{cases}$$

解： $M = 5 \times 6 \times 7 \times 11 = 2310$

$M_1 = \frac{2310}{5} = 462$，　$M_2 = \frac{2310}{6} = 385$，　$M_3 = \frac{2310}{7} = 330$，　$M_4 = \frac{2310}{11} = 210$

$462y_1 \equiv 1 (\bmod 5)$，　$385y_2 \equiv 1 (\bmod 6)$，　$330y_3 \equiv 1 (\bmod 7)$，　$210y_4 \equiv 1 (\bmod 11)$

$462 = 92 \times 5 + 2$，　$2 = 462 - 92 \times 5$

$5 = 2 \times 2 + 1$，　$1 = 5 - 2 \times 2 = 5 - 2 \times (462 - 92 \times 5) = 93 \times 5 - 2 \times 462$

$y_1 \equiv 462^{-1} (\bmod 5) \equiv -2 \equiv 3 (\bmod 5)$

$385 = 64 \times 6 + 1$，　$1 = 385 - 64 \times 6$，　$y_2 \equiv 385^{-1} (\bmod 6) \equiv 1$

$330 = 47 \times 7 + 1$，　$1 = 330 - 47 \times 7$，　$y_3 \equiv 330^{-1} (\bmod 7) = 1$

$210 = 19 \times 11 + 1$，　$1 = 210 - 19 \times 11$，　$y_4 \equiv 210^{-1} (\bmod 11) = 1$

$x = 3 \times 462 + 385 \times 5 + 330 \times 4 + 210 \times 10 = 6731 \equiv 2111 (\bmod 2310)$

1.8　Gauss 算法

$x \equiv a_i (\bmod n_i) (i = 1, 2, \cdots, k)$，$n_1, n_2, \cdots, n_k$两两互素，$n = \prod_{i=1}^{k} n_i$，则

$$x = \sum_{i=1}^{k} a_i N_i M_i (\bmod n)$$

式中，$N_i = \frac{n}{n_i}$；$M_i = N_i^{-1} (\bmod n_i)$。

例 1-14　求解下式。

$$\begin{cases} x \equiv 2 (\bmod 3) \\ x \equiv 3 (\bmod 5) \\ x \equiv 2 (\bmod 7) \end{cases}$$

其中：$n_1=3$、$n_2=5$、$n_3=7$、$n=105$；$N_1=\frac{105}{3}=35$、$N_2=21$、$N_3=15$。$M_i=N_i^{-1}(\bmod n_i)$，$M_1=35^{-1}(\bmod 3)$。

解：$35=11\times3+2\quad 3=2+1$

$1=3-2=3-(35-11\times3)=12\times3-35$

$M_1=35^{-1}(\bmod 3)=-1=2$

$M_2=21^{-1}(\bmod 5)$

$21=4\times5+1\quad 1=21-4\times5\quad 21^{-1}(\bmod 5)=1=M_2$

$M_3=15^{-1}(\bmod 7)$

$15=2\times7+1\quad 1=15-2\times7\quad 15^{-1}(\bmod 7)=1$

$M_3=15^{-1}(\bmod 7)=1$

$x=2\times35\times2+3\times21\times1+2\times15\times1=140+63+30=233\equiv23(\bmod 105)$

1.9　古典密码举例之一：Kaiser 密码

古典密码，简单地说就是收信方和发信方二人间秘密传递信息的技术。信息 m 经过某种变换成为密码 $E_k(m)$，这个密码也只有通信双方能读懂，其他人一般无法了解，其中参数 k 称为密钥，$E_k(m)$称为密文，记为 $C=E_k(m)$。

算法确定后，由于密钥 k 的不同，密文也就不一样，密钥 k 也只有有关通信的双方保管掌握，如图 1-1 所示。

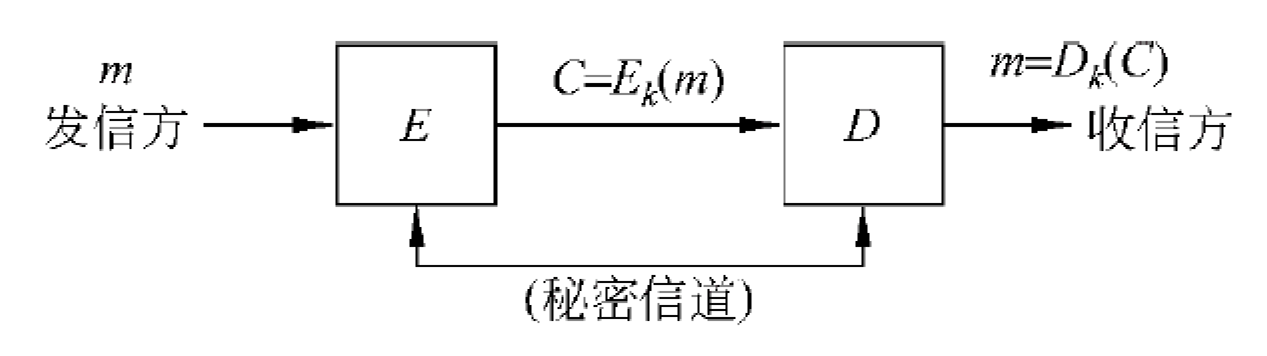


图 1-1　加密图示

密钥 k 通过秘密信道传输，即由通信双方秘密约定。E 表示加密算法，$C=E_k(m)$ 是密文，D 是 E 的逆运算，即解密。

例 1-15　明文 m 是 Secure message transmission is of extreme importance in information based society

解：其明文的意义是"在信息社会，信息的秘密传输是极其重要的"。最早的一个称为 Kaiser 密码的，以英文 26 个字母分别对应于数字 0～25。如下：

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

明文和密文间的变换公式是：

$$C\equiv m+k(\bmod 26)$$

密钥 k 是 0～25 间的整数，例如取 $k=10$，则与上面信息 m 对应的密文便是：

C O M E B O W O C C K Q O D B K X C W S C C S Y X S C Y
P O H D B O W O S W Z Y B D K X M O S X S X P Y B W Z D

S Y X L K C O N C Y M S O D I

Kaiser 密码是恺撒大帝在战争中首次应用的密码，虽然用今天的眼光来看是不堪一击的，但在当时是一大发明。

1.10 古典密码举例之二：单表置换

下面介绍古典密码中很有趣的一种加密算法，密钥 k 不是一个整数，而是一个词组，比如密钥 k 是：future belongs to efficiency 词组的意义是“未来属于效率”，由此得一单表置换如下：

a b c d e f g h i j k l m n o p q r s t u v w x y z
F U T R E B L O N G S I C Y A D H J K M P Q V W X Z

首先介绍 FUTREBLONGSICYAD…Z 的组成原则，密钥词组：future belongs to efficiency，按顺序 FUT 后面的 U 前面已出现不再重复，故得 FUTREBLONGSICY，后面跟上英文字母按顺序续上前面未出现的字符：ADHJKMPQVWXZ。

密码设计要使计算 $E_k(C)$ 比较容易，但不知 k 时要破解密文则要尽可能困难，词组密码的破译远比 Kaiser 密码困难得多。若没有好的方法则可采用穷举法来强行攻击，考虑到单表置换表实际上是 26 个英文字母的一个全排列。

根据

$$n! \approx \sqrt{2n\pi}\left(\frac{n}{e}\right)^n \quad \sqrt{2\times 26\times\pi}\left(\frac{26}{e}\right)^{26} = 12.781\times 3.1452\times 10^{25} = 4.02\times 10^{26}$$

若用每秒能进行 100 万个方案判定的计算机来进行计算，需要的机器时间为

$$T = \frac{4.02\times 10^{26}}{365\times 24\times 3600\times 10^6} = \frac{4.02\times 10^{26}}{3.1536\times 10^{13}} = 1.275\times 10^{13}\text{(年)}$$

可见，强行攻击是不可行的。

Kaiser 密码属于单表置换，下面举一个用单表置换的密码进行分析的例子。已知密文：

GJXXN GGOTZ NUCOT WMOHY JTKTA MTXOB
YNFGO GINUG JENSZV QHYNG NEAJF HYOTW
GOTHY NAFZN FTUIN ZBNEG NLNFU TXNXU
FNEJC INHYA ZGAEU TUCQG OGOTH JOHOA
TCJXK HYNUV COCHO UHCNU GHHAF NUZHY
NCUTW JUWNA EHYNA FOWOT UCHNP HOGLN
FQZNG OFUVC NVJHT AHNGG NTHOU CGJXY
OGHYN ABNTO TWGNT HNTXN AEBUF KNFYO
HHGIU TJUCE AFHYN GACJH OATAE IOCOH
UFQXO BYNFC

明文经过单表置换加密变得面目全非，但单表置换还是留下了原文的某些“基因”可供利用。分析方法并不困难，也没用到什么“高等数学”，而且方法饶有趣味，对密文应该

注意什么，颇有助益。

经统计，英文书籍和报刊中各英文字母出现的频率惊人得接近，例如 e 出现的频率总是最高，t、a、o、n、i 也较高；连缀字也有类似的情况，th、he、in、er、an、re、ed、on、es、st、en、at、to、ne、ha、nd、oa、ea、ng、as、or、ti、is、et、it、ar 等经常出现；3 个连缀字为 the、ing、and、her 等。下面将 26 个字母出现的频率列表如表 1-3 所示。

表 1-3　单个字母出现的频率

英文	a	b	c	d	e	f	g	h	i
频率	0.0856	0.0139	0.0279	0.0378	0.1304	0.0189	0.0199	0.0528	0.0627
英文	j	k	l	m	n	o	p	q	r
频率	0.0013	0.0042	0.0339	0.0249	0.0707	0.0799	0.0199	0.0012	0.0677
英文	s	t	u	v	w	x	y	z	
频率	0.0607	0.1045	0.0249	0.0092	0.0149	0.0092	0.0199	0.0008	

从表中可以看出如下特点。

(1) e 的频率最高，接下来是 t、a、o、n、r、i、s、h，这些属于高频部分。

(2) d、l、u、c 属中频部分。

(3) d、f、y、w、g、b、v 属低频部分。

(4) k、j、x、q、z 属超低频部分。

(5) 各部分的分隔比较明显，例如高频中频率最低的 h，比中频中频率最高的 d 相差的频率为 0.0528－0.0378＝0.015。

(6) e 的频率最高，比次高的 t 的频率高出 0.1304－0.1045＝0.0259。

现在回到对 280 个密文字母出现的数目进行统计，如下：

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
16	5	13	6	7	17	23	26	5	12	3	2	2	36	25	1	5	0	0	22	20	4	6	9	14	7

若按频率从大到小排列有：

N	H	O	G	T	U	F	A	Y	C	J	X	E	Z	D	W	B	I	Q	V	K	L	M	P	R	S
36	26	25	23	22	20	17	16	14	13	12	9	7	7	6	6	5	5	5	4	3	2	2	1	0	0

容易做出判断的是 N↔e。

高频部分的 9 个字母：N、H、O、G、T、U、F、A、Y 可能是 e、t、a、o、n、i、r、s、h 的某种对应，N↔e 是肯定的。

如果将高频的 9 个字符之间的明密对应，确定 9 个字符占 280 密文中的 199 个，占全部字符的 0.71。

现将前面 9 个高频字母之间的连缀关系列表如表 1-4 所示，以帮助确定各自对应的明文字母。例如 e↔N 确定后，从 eA 的频率高于 ae、he 连缀的频率高于 eh 的频率等，可以确定哪个字母对应于 A，哪个字母对应于明文 h，哪个字母对应于明文 t……

表 1-4　9 个高频字母之间的连缀关系

↓ →	N	H	O	G	T	U	F	A	Y	明文
N		3 1		4 5	 4	 5	3 7	 5	9 	e
H	1 3	2 2	5 4	2 1	4 1	1 1	2 	1 1	 10	
O		5 4		6 10	1 7	 1	1 1	 2		i
G	5 4	2 1	4 6	2 2		2 	2 	 2		?
T	4 	1 4	7 1			4 3	1 	2 3		n
U	5	1 1	1 	 2	3 4	2 3				a
F	7 3	 2	1 1	 3	 1	3 2		3 	 1	?
A	5 	1 1	2 	2 	3 2		 4		1 	o
Y	 9	10 	 3				1 	1 		h

表中有上下两数，以 N 行 G 列的$\begin{pmatrix}4\\5\end{pmatrix}$为例，即 280 个密文字符中出现 GN 连缀的有 4 次，出现 NG 连缀的有 5 次，N 行 Y 列的$\begin{pmatrix}9\\ \ \end{pmatrix}$即为$\begin{pmatrix}9\\0\end{pmatrix}$，说明 NY 出现 9 次，没有出现 YN。

现在根据统计的数据依次作出如下判断。

(1) N 是 e 的密文，用 N↔e 表示，大写为密文，小写为明文。

(2) 高频字母 a、i、o 这三个字母两两连缀的机率较少，从表中可见 O、U、A 三个字母两两连缀数稀少，初步判断它们可能是 a、i、o 的密文，但不能确定如何对应。

(3) a、i、o 的连缀机会很少，但 io 的连缀机率(0.0893)比 io 的连缀机率(0.0092)高，从表中看到 OA 出现两次，OU 出现一次，UO、UA、AO、AU 均为空，所以 OA 可能是 io 的密文，即 O↔i，A↔o。

(4) U 可能是 a 的密文，OU 出现 1 次、NU 出现 5 次、UN 不出现，符合 ea 出现的频率(0.066)高于 ae 出现的频率(0.002)，所以 U↔a 的可能性很大。

(5) 根据统计 n 前面是母音的频率分别为 an 的频率(0.1878)、en 的频率(0.1381)、in 的频率(0.2498)、on 的频率(0.219)、un 的频率(0.1517)，n 前面母音的频率高达 0.90 以上，故 T↔n。

(6) Y 的特点也很突出，YN 出现 9 次，而 NY 不出现，与 he 出现的频率(0.5623)远高于 eh 出现的频率(0.0021)吻合，所以 Y↔h 的可能性很大。

(7) th 出现的频率为 0.3512，ht 出现的频率仅为 0.0233，所以可能 H↔t。

(8) 高频字母中 r、s 尚难作出判定，初步作出 280 个密文字母中的 159 个的判定，占 57%，先将初步结果代入密文，进行观察：

GJXX N GG OT Z NU CO TW MOHY J T K TAMT XO B YN FGO GI NU GJFN ZVQ HYN GN EA JFHY OTW
e in ea i with n nown i he i es e the e o in-

G OTHYNA FZ N F TU I N ZB N FG N L N F UT XN XU F N EJ CI NHYA ZGA E UTU CQGO G OTHJOHOAT
intheo e na e e e e an e a e etho o ana i intuition

CJXK HYNU VO CO HQ UH C NU G HHA F NU ZHY
thea i i at ea tto ea h

继续判定如下。

(9) MOHY 可能是 with 的密文，故 M↔w。

(10) 根据 J T K TAMT 和 O G OTH J OHOAN 可猜出 J↔u，K↔k。
n nown i int itio

(11) 将新的判定再代入密文与明文的单表置换得

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
U				N			Y	O		K			T	A					H	J		M			

可得 L↔v。

(12) 由(8)知 F 和 G 可能和 r、s 对应，现由于 H↔t、J↔u，故 F↔r，G↔s。

(13) 由于 U↔a，故 V↔b。

(14) 再代入密文，得

GJXXNGG OT Z NU C OT W MOHYJTKTAMT XOBYNFGOG I NUGJFN Z V Q HYNGN E AJF HYOTW
su ess in ea in withunknown i hers is essure b these our thin

(15) 由 suXXess 可定 X↔c。

(16) 由 CiBhers 可得 B↔p。

(17) 由 thinW 可令 W↔g。

由此得密钥词组为 New york city，得置换表为

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
U	V	X	Z	N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S

全部明文为

Success in dealing with unknown ciphers is measured by these four things in the order named perseverance, careful methods of analysis, intuition, luck. The ability at least to read the language of the original text is very desirable but not essential. Such is the opening sentence of Parker Hitt's manual for the Solution of Military Ciphers.

标点是加上去的，原文很有意思：“破译一未知密码是否成功，可以由以下 4 个因素来衡量，按其顺序为毅力、审慎的分析方法、直观和运气。阅读原文的文字的起码能力是需要的，然而不是必不可少的。这是 Parker Hitt 的《军事密码破译指南》一书的开场白”。

作为古典密码的单表置换，在今天已成历史，但它揭示了一个重要的事实，好的加密算法绝不留给统计以空间。

1.11　古典密码举例之三：Vigenere 密码

设 $M=m_1m_2\cdots m_n$、$k=k_1k_2\cdots k_n$、$E_k(m)=c_1c_2\cdots c_n$，则 $c_i=m_i+k_i \pmod{26}$ $(i=1,2,\cdots,n)$。

比如 $M=$data security，$b=$best，则 $c=E_k(m)=$EELT TIUN SMLR。

```
   data        secu        rity
+) best     +) best     +) best
   EELT        TIUN        SMLR
```

还是以 $m=$secure message transmission is of extreme importance in information society 为例。

$k=$security，先将 m 分成 8 个字符一节：

securemе　ssagetra　nsmissio　nisofext　remeimpo

rtancein　informat　ionbased　society

```
   secureme                 ssagetra
+) security              +) security
   KIEOIMFC  (mod 26)       KWCAVBKY  (mod 26)
   nsmissio                 remeimpo
+) security              +) security
   EWOCJABM  (mod 26)       JIOYZUIN  (mod 26)
   rtancein                 informat
+) security              +) security
   JXCHTMBN  (mod 26)       ARHIJUIS  (mod 26)
   ionbased                 society
+) security              +) securit
   ASPVRSXB  (mod 26)       KSECVER  (mod 26)
```

所以得密文：

KIEOIMFCKWCAVBKYEWOCJABMJIOYZUISJXCHTMBNARHIJUISASPVRIXBKSECVER

Vigenere 密码摆脱了单表置换的弱点，但仔细分析还是有一些统计特性无法摆脱，终于被破译了。本文不准备完全地解剖到底，仅提供几个很有趣的线索进一步探讨。

（1）首要的问题是关于密钥 k 的长度的确定。密钥 k 的长度可以从密文中找到线索，英文的连缀字有很多，如 th、he…不计其数，三连缀的也不少。这么多的连缀字难免其中两个的距离是 k 的长度的倍数，只要距离是 k 的长度的倍数，则它们的密文将是相同的。所以从密文中查找相同连缀字的数目入手，并求其中的距离，从距离中可推测出密钥 k 长度的倍数。k 的长度不可能很大或很小，如 2 或 3，可从因数分解距离统计因数的次来推断密钥的长度。

（2）当密钥确定之后，依次将密文分成 1、2、…、k 个子集，每个子集的元素间的距离都是 k 的倍数。请读者注意，这样的 k 段各自都可以看作是英文作 mod $26+h$ 的单表变

换而成的。它自然保留有英文的“基因”不变。

前面已给出 26 个英文字母的频率表，比如 $f_a=0.0856$、$f_b=0.0139$…在一段英文中任意两处出现相同字母的概率为

$$p=f_a^2+f_b^2+\cdots+f_z^2=(0.0856)^2+(0.0139)^2+\cdots+(0.0008)^2=0.0687$$

加密过程是按密钥 k 分成 k 部分，相当于列队时报数为 1 的向前走 k_1 步，报数为 2 的向前走 k_2 步，…，报数为 h 的向前走 k_h 步，k 行就是这样形成的。现在要判断各行要向前各走多少步才能恢复原始的队列，下面引进一概念“重合指数 IC”。

令 $\mathrm{IC}=\sum_{\xi=A}^{i} n_\xi \dfrac{n_\xi-1}{n(n-1)}$，IC 很明显是任意两处是同样字符的概率，这个值越接近 0.0687，说明其越接近“英文”原型。

Vigenere 密码是将原文分成 k 段，如果能将 k 段两两地配合，使之联合起来使 IC 接近 0.0687，从两两配合到整体划一的 IC 达到 0.0687。

请读者仔细思考如何从两段的密文配合求联合的 IC，及最后如何求出密钥。

假如已知密文：

UFQUIUDWFRGLZARIHWLLWYYFSYYQATJJPFKMUXSSWWCSVFAEVWWGQCM
VVSWFKUTBLLGZFVITYOEIPASJWGGSJEPNSUETPTMPOPHZSFDCXEPLZQWKD
WFXWTHASPWIUOVSSSFKWWLCCEZWEUEHGVGLRLLGWOFKWLUWSHEVWST
TUARCWHWBVTGNITJRWWKCOTFGMILRQESKWGYHAENDIULKDHZIQASFMPR
GWRVPBUIQQDSVMPFZMVEGEEPFODJQCHZIUZZMXKZBGJOTZAXCCMUMRSSJW

字符数为 280，A：9 个、B：4 个、C：10、D：7 个、E：14 个、F：15 个、G：14 个、H：10 个、I：11 个、J：7 个、K：9 个、L：13 个、M：10 个、N：3 个、O：7 个、P：12 个、Q：9 个、R：8 个、S：20 个、T：12 个、U：14 个、V：12 个、W：27、X：5 个、Y：6 个、Z：12 个。

IC＝0.431。显然离 0.0687 还远。

从密文中查相同的连缀字，比如 IU 有三处，距离为 118、203、259，UI 有一处距离 225……

对每一个距离进行因数分解，比如 250＝2×5×5×5。

统计结果 2：52 次、3：32 次、4：28 次、5：50 次……

2 太短，3、4 也短而且出现次数不多，故判定密钥长度为 5。将密文分为 5 行：

U U G I W　Y J U W A G V U G T F G P T O F P K W P V K C
U G G W H　T C V T K G Q G N K Q P V Q M V P Q U K O C R

$$\mathrm{IC}=0.0623$$

F D L H Y　Y P X C E Q S T Z Y A G N P P D L D T W S W E
E L W L E　T W T J C M E Y D D A R P Q P E C Z Z T C S

$$\mathrm{IC}=0.0506$$

Q W Z W Y　Q F S S V C W B F O S S S T H C Z W H I S W Z
H R O U V　U H G R O I S H I H S G B D F G O H Z B Z M S

$$\mathrm{IC}=0.0649$$

U F A L F　A K S V W F L V E J J U M Z X Q F A U S L W
G L F W W　A W N W T L K A U Z F W U S Z E D Z M G A U J

IC = 0.0617

V H R L S T M W F W V K L I I W E E P S E W X S G F C E
V L K S S R B I W P R W E L I M R I V M E J I X J X M W

IC = 0.0617

每一行相邻两个字母都是密文中距离为 5，从 5 个 IC 来看，密钥 k 长为 5 的判断很正确。

假定 $k=k_1k_2k_3k_4k_5$，第 1 行是作 $m+k_1 \pmod{26}$ 置换而得、第 2 行是作 $m+k_2 \pmod{26}$ 置换而得、第 3 行是作 $m+k_3 \pmod{26}$ 置换而得、第 4 行则为作 $m+k_4 \pmod{26}$ 而得、第 5 行则为作 $m+k_5 \pmod{26}$ 置换而得。

$1\leqslant k_i\leqslant 26(i=1,2,3,4,5)$。假如 $k_1=1$，如何选择 k_2、k_3、k_4、k_5，使最后结果的 IC 最大？留给读者思考，并请读者检验 $k_1=1$、$k_2=9$、$k_3=12$、$k_4=16$、$k_5=2$ 是最后结果。

1、9、12、16、2(mod 26) 的模式有：

AJMOD BKNRD CLOSE DMPTF ENQUG…
… XGJNZ YHKOA ZILPD

显然密钥是 CLOSE。

将 5 段密文连接得

U W E E G U U K P F G C N K P I Y K V J W P M P Q Y P E
K R J G T U K V O G C U W T G F D A V J G U G H Q W T V
J K P I U K P V J G Q T F G T P C O G F R G T U G X G T
C P E G E C T G H W N O G V J Q F U Q H C P C N A U K U
K P V W K V K Q P N W E M V U G C D K N K V A C V N G C
U V V Q T G C F V J G N C P I W C I G Q H V J G Q T K I
K P C N V G Z V K U X G T A F G U K T C D N G D W V P Q
V G U U G P V K U N U W E J K U V J G Q R G P K B I U G
P V G P E G Q H R C T M G T J K V V U O C P W C N H Q T
V J G U Q N W V K Q P Q H O K N K V C T A E K R J G T U

统计 26 个英文字母出现的次数：

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	0	26	4	5	7	36	7	6	14	25	0	3	13	5	22	16	5	0	17	23	26	12	2	2	1

IC = 0.0654

由此，密文可以确定为下面的明文通过恺撒变换加密而成：

Success in dealing with unknown ciphers is measured by these four things in the order named perseverance, careful methods of analysis, intuition, luck. The ability at least to read the language of the original text is very desirable but not essential. Such is the opening sentence of Parker Hitt's manual for the Solution of Military Ciphers.

这已见于前面。

1.12 Wilson 定理与 Fermat 定理

定理 1-15：p 是素数的充要条件是$(p-1)!\equiv -1(\bmod\ p)$。

证 必要条件 $p=2$ 时，$(p-1)!\equiv 1\equiv -1(\bmod\ 2)$，定理在 $n=2$ 时成立。

假定 p 为大于 2 的素数，a 是满足 $1\leqslant a\leqslant p-1$ 的整数，因$(a,p)=1$，故存在 l 和 m，使 $la+mp=1$、$la\equiv 1(\bmod\ p)$，即 $a^{-1}\equiv l(\bmod\ p)$。而且 $1^{-1}(\bmod\ p)\equiv 1$，$(p-1)^{-1}\equiv p-1(\bmod\ p)$，所以 2、3、…、$p-2$ 可分成为$(p-2)/2$ 对$(\bmod\ p)$的互递。即 $2\times 3\times\cdots\times(p-2)\equiv 1(\bmod\ p)$。

所以

$$(p-1)!=1\times 2\times\cdots\times(p-2)(p-1)\equiv(p-1)(\bmod\ p)\equiv -1(\bmod\ p)$$

充分条件 已知$(p-1)!\equiv -1(\bmod\ p)$，但 $p=ab$，其中 $1<a<p$，$1<b<p$，因 $a<p$，故 $a\mid(p-1)$，根据 $p-1\equiv -1 \bmod p$，$(p-1)+1\equiv 0 \bmod p$，所以，$p\mid[(p+1)!+1]$，即 $a\mid[(p-1)!+1]$，由$[(p-1)!+1]-[p-1]!=1$，可知，$a\mid 1$ 与 $a>1$ 的假设矛盾，故 p 是素数。

证毕

Wilson 定理是判定 n 是素数的充要条件，不过 n 很大时，计算量太大，不实用。

定理 1-16（Fermat 定理）：p 是素数，a 是正整数，$p\nmid a$，则 $a^{p-1}\equiv 1(\bmod\ p)$。

证 $p-1$ 个整数 a、$2a$、…、$(p-1)a$ 中无一被 p 除尽。

$a,2a,\cdots,(p-1)a$ 不存在一对$(\bmod\ p)$同余，因若 $ha\equiv ka(\bmod\ p)$，$1\leqslant h<k\leqslant(p-1)$，$(a,p)=1$，则 $h\equiv k(\bmod\ p)$。这是不可能的。

所以 a、$2a$、…、$(p-1)a$ 这 $p-1$ 个整数 mod p 不和 0 同余，不存在两个互相同余，其结果形成 mod p 的简化剩余集。

故

$$a\cdot 2a\cdots(p-1)a\equiv 1\times 2\times\cdots\times(p-1)(\bmod\ p)$$
$$a^{p-1}(p-1)!\equiv(p-1)!(\bmod\ p)$$
$$((p-1)!,p)=1\quad \text{所以 } a^{p-1}\equiv 1(\bmod\ p)$$

证毕

Fermat 定理给出素数 p 的必要条件。

定理 1-17：p 是素数，a 是正整数，则 $a^p\equiv a(\bmod\ p)$。

证 若 $p\nmid a$，则根据 Fermat 定理：$a^{p-1}\equiv 1(\bmod\ p)$，则 $a^p\equiv a(\bmod\ p)$，若 $a\mid p$，则 $p\mid a^p$，$a^p\equiv a\equiv 0(\bmod\ p)$。

利用 Fermat 定理可简化 $a^n(\bmod\ p)$的运算。

例 1-16 求 $5^{109}(\bmod\ 9)$。

解：根据 Fermat 定理，$5^8\equiv 1(\bmod\ 9)$、$101=8\times 12+5$，所以 $5^{101}=(5^8)^{12}\times 5^5\equiv 5^5\equiv 3125\equiv 2(\bmod\ 9)$。

定理 1-18：p 是素数，$p\nmid a$，则 $a^{-1}(\bmod\ p)\equiv a^{p-2}$。

证 $a\cdot a^{p-2}=a^{p-1}\equiv 1(\bmod\ p)$，所以 $a^{p-2}\equiv a^{-1}(\bmod\ p)$。

例 1-17　求 5^{-1}(mod 11)。

解：$5^9=1\,953\,125\equiv 9$(mod 9)，故 5^{-1}(mod 11)$=9$。

例 1-18　求解 $ax\equiv b(\text{mod } p)$，已知 $p\nmid a$，a，b 是整数，p 是素数。

解：$x\equiv a^{b-2}b(\text{mod } p)$

1.13　Euler 定理

定义 1-4：n 是正整数，不超过 n 与 n 互素的正整数数目用 $\phi(n)$表示，称为 Eulerϕ 函数。

例如 $\phi(1)=1$、$\phi(2)=1$、$\phi(3)=2$、$\phi(4)=2$、$\phi(5)=4$、$\phi(6)=2$、$\phi(7)=6$、$\phi(8)=4$，因 $(1,n)=1$，1 和任何整数互素。

每一个整数 mod n 总和 0、1、2、…、$n-1$ 中的一个数同余，而且仅和其中一个数同余，0、1、2、…、$n-1$ 便称为 mod n 的一组完全的正剩余系。

mod n 和 r 同余的数的集合表示为[r]，r 中的每一个数可表示为 $r+kn(k=0,\pm 1,\pm 2,\cdots)$。

[r] 类中每一个数和 n 互素的充要条件是$(r,n)=1$，mod n 有 $\phi(n)$ 个与 n 互素的同余类。从这 $\phi(n)$ 个同余类中各取一个组成的集合称为简化的剩余类。

定理 1-19：若 m_1 和 m_2 互素，则 $\phi(m_1m_2)=\phi(m_1)\phi(m_2)$。

证　设 x 是一正整数，$0\leqslant x<m_1m_2$。

$$x\equiv r_1(\text{mod } m_1)\quad 0\leqslant r_1<m_1$$
$$x\equiv r_2(\text{mod } m_2)\quad 0\leqslant r_2<m_2$$

r_1 和 r_2 为 x 所唯一确定，即 x 和(r_1,r_2) 一一对应。

x 和 m_1m_2 互素，当且仅当 x 和 m_1、m_2 都互素，x 和 m_i 互素的充要条件是 r_i 和 m_i 互素$(i=1,2,\cdots)$。

这就证明了与 m_1m_2 互素的数目等于数偶(r_1,r_2) 的数目，其中 r_1 和 m_1 互素，r_2 与 m_2 互素，比 m_i 小而与 m_i 互素的数的数目为 $\phi(m_i)(i=1,2,\cdots)$，故(r_1,r_2) 的数目为 $\phi(m_1)\phi(m_2)$。

定理 1-20：若 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，其中 p_i 是不同的素数，$\alpha_i\geqslant 0(i=1,2,\cdots,k)$，则

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

证　首先证当 p 是素数时 $\phi(p^\alpha)=p^\alpha\left(1-\dfrac{1}{p}\right)$。

在区间 $0\leqslant x<p^\alpha$ 上的整数，其中是 p 的倍数的有：0、p、$2p$、…、$(p^{\alpha-1}-1)p$，共 $p^{\alpha-1}$个。其余都与 p^α 互素，所以小于 p^α，而与 p^α 互素的数的数目为

$$p^\alpha-p^{\alpha-1}=p^\alpha\left(1-\frac{1}{p}\right)$$

由于 $\phi(m_1m_2)=\phi(m_1)\phi(m_2)$，$m_1$ 和 m_2 互素，故若 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

定理 1-21（Euler 定理）：若 a 与 m 互素，则 $a^{\phi(m)} \equiv 1(\bmod m)$。

证　设 $\phi(m)=k$，令 r_1、r_2、…、r_k 是与 m 互素的 mod m 的剩余集，由于$(a,m)=1$，所以 $ar_1, ar_2, \cdots, ar_k$ 也与 m 互素，且 mod m 互不同余。如若不然，存在 $r_i \neq r_j$，而 $ar_i \equiv ar_j(\bmod m)$，存在 $a^{-1}(\bmod m)$，使 $r_i \equiv r_j(\bmod m)$，与假设矛盾。所以 $a^k r_1 r_2, \cdots, r_k \equiv r_1, r_2, \cdots, r_k(\bmod m)$。

由 r_1、r_2、…、r_k 两两互素，所以

$$a^k \equiv 1(\bmod m) \quad 即 \quad a^{\phi(m)} \equiv 1(\bmod m)$$

Fermat 定理：若$(a,b)=1$，则 $a^{p-1}=1(\bmod p)$。可见 Fermat 定理是 Euler 定理的特例。

例 1-19　$\phi(100)=\phi(2^2 5^2)=100\times\left(1-\frac{1}{2}\right)\times\left(1-\frac{1}{5}\right)=40$。

1.14　Euler 定理帮助人们完成了一场密码学的革命

前面介绍的古典密码，通信双方的密钥由双方私下约定，所以加密用的密钥和解密用的密钥是一样的，也可以形象地说是对称密码体制。这使得军事或政治上矛盾不突出，多半是单线联系。但到网络时代，信息本身就是财富，人们迫切需要密码。以银行为例，和它保密通信的用户成千上万。若通信双方用的密钥由双方约定，其数目将不胜其数，密钥也要定期更换，这些都是不胜其烦的工作。每个与银行保持通信的人和机构比较多的是将两两约定的密钥记录在计算机系统或私人的保密本上，这样做本身就极不安全。

Diffie 和 Hellman 于 20 世纪 70 年代发表了《密码学的新方向》的文章，提出公钥密码的新思想。假定每个用户（设为 A）有一加密用的密钥 k_A，不同于解密用的密钥 k_A^*，A 将 k_A 公开，将 k_A^* 保密，当然要求将 k_A 公开不至于影响到 k_A^* 的安全。B 欲与 A 保密通信信息 m，B 查到 A 的公钥 k_A，并且 k_A 加密得密文 $C=E_{k_A}(m)$。并将 C 送给 A，A 用只有他掌握的解密密钥 k_A^* 解密得 $m=D_{k_A^*}(C)$。

由于解密密钥 k_A^* 只有 A 自己掌握，任何第三方截获密文 C，均无法恢复明文 m。如果有这样的公钥，加密用的密钥不同于解密密钥，与古典密码的密钥对称性相区别，称公钥密码为非对称密码。

其实 Diffie 和 Hellman 发表他们的公钥思想时还只是一种设想，还没有真正意义上的公钥的实现，但他们建议：每个用户（设为 A），从集合 $P=\{1,2,\cdots,p-1\}$ 中任取一元素 x_A，计算 $y_A \equiv b^{x_A}(\bmod p)$，其中 b 是约定的本原元素，A 将 y_A 公布，x_A 保密。已知 y_A 求 x_A 是解一离散对数问题（后面将讨论到它，是一道难题）。B 欲与 A 保密通信，查到 A 的公钥 y_A，计算通信密钥：

$$\begin{aligned} k_{AB} &\equiv (y_A)^{x_B} \equiv \bmod p \equiv (b^{x_A})^{x_B} \bmod p \equiv b^{x_A x_B} \bmod p \equiv ((y_b)^{x_A}) \bmod p \\ &\equiv b^{x_A x_B} \bmod p \end{aligned}$$

但这只是解决双方通信密钥，而实现通信还是利用对称密码，其中 b 是 mod p 的本原元素，有时也叫作原根，即 $b^{p-1}=1(\bmod p)$。而且当 $k=1,2,\cdots,p-1$ 时，$b^k \bmod p$ 形成了 mod p 的正剩余系数，p 是一素数。

由于 Diffie 和 Hellman 的思想富有革命性，使得各国的密码学家为之倾倒，很快就有第一个公钥密码诞生，第二个紧接着到来，甚至于难分第二还是第一，几乎是同时产生。下面先介绍 RSA 公钥密码。

RSA 是它的三个发明者 Rivest、Shamir 和 Adleman 的缩写。RSA 密码基于 Euler 定理，它的加密过程是每个用户（设为 A）做以下操作。

（1）选取两个素数 q_A 和 p_A。

（2）计算 $n_A=p_Aq_A$（公开），$\phi(n_A)=(p_A-1)(q_A-1)$（保密）。

（3）随机地选一整数 e_A，使其满足 $(e_A,\phi(n_A))=1$（公开）。

（4）计算 d_A 满足 $e_Ad_A\equiv 1(\bmod\ \phi(n_A))$（保密）。

RSA 系统的所有用户（如 A），将 e_A、n_A 全部公开。

用户 B 欲与 A 保密通信可查到 e_A 和 n_A，B 将明文 m 取长度小于 $\log_2 n$ 位的数字作为明文块。

加密过程：密文 $C\equiv m^{e_A}(\bmod\ n_A)$，$B$ 将 C 送给 A，A 收到 C 后作 $D(C)\equiv C^{d_A}(\bmod\ n_A)$。下面将计算 $m=D(C)$，对任何整数 k 及 m，$m<n_A$，恒有 $m^{k\phi(n_A)+1}\equiv m(\bmod\ n_A)$。

若 $(m,n_A)=1$，则 $m^{\phi(n_A)}\equiv 1(\bmod\ n_A)$。

$$C\equiv m^{e_A}(\bmod\ n_A)\quad C^{d_A}(\bmod\ n_A)\equiv(m)^{e_Ad_A}(\bmod\ n_A)$$

$$e_Ad_A\equiv 1(\bmod\ \phi(n_A)),$$

故

$$D(C)\equiv m(\bmod\ n_A)$$

由于 d_A 是保密的只有 A 自己掌握，所以只有 A 自己才能解密，当然明文 m 必须数字化，比如英文字母可用它的序号，例如 $p=43$、$q=59$、$n=43\times 59=2537$，$\phi(n)=42\times 58=2436$，取 $e=13$。

$$2436=187\times 13+5\quad 13=2\times 5+3\quad 5=3+2\quad 3=2+1$$

$$1=3-2=3-(5-3)=2\times 3-5=2\times(13-2\times 5)-5=2\times 13-5\times 5$$
$$=2\times 13-5\times(2436-13\times 187)=937\times 13-5\times 2436$$

所以 $d=937$，$937\times 13\equiv 1(\bmod\ 2436)$。

若明文为 public key encryptions，将明文分块为

pu bl ic ke ye nc ry pt io ns

明文数值化为

1520 0111 0802 1004 2404 1302 1724 1519 0814 1418

加密得密文：

0095 1048 1410 1299 1365 1379 2333 0132 1751 1289

比如 $1520^{13}(\bmod\ 2539)\equiv 0095$，其他照此不再细述。这里要回答一个问题 $n=pq$（公开），$\phi(n)=(p-1)(q-1)$（保密）能做得到吗？RSA 密码是建立在大数因子分解的困难性上的，一般 $n=pq$ 约 1024 位，甚至更多，十进制数约三百多位，p 和 q 的十进制数都是一百多位。

接着又派生出新的问题：如何判定一百多位十进制数的素数？如何分解三百多位的十进制数？如此问题便成为研究的核心问题，而且水涨船高，一浪高过一浪，比如 1990 年

150 位的 F_9 被因数分解成功,F_9是第 9 个 Fermat 数,1999 年被称为 RSA155 的 155 位数为

n =10 941 738 641 570 527 421 809 707 322 040 357 612 003 732 945 449 205 990 913 842
131 476 349 984 288 934 784 717 997 257 891 267 332 497 625 752 899 781 833 797
016 537 244 027 146 743 531 593 354 333 897

p =10 263 959 282 974 110 577 205 419 657 399 167 590 071 656 780 803 806 680 334
193 352 179 071 130 779

q = 106 603 488 380 168 454 820 927 220 360 012 578 679 207 958 575 989 291 522 270
608 237 193 062 808 643

总之,大数的分解技术在提高,判定素数的办法也在变化,这些都是研究数论者责无旁贷的。后面将围绕这些问题展开。

1.15 数字签名

RSA 密码还有一项十分突出的功能,即"数字签名"。其重要性一点也不低于它的加密算法,在网络时代的通信中,特别是有关金融、商业等交往中所必需的。比如 A 向 B 承诺的事,口说无凭,写一书面文件,以往 A 需在书面文件上签名盖章,如果时过境迁,A 反悔,不承认有这项约定,B 可持此书面文件去法院处理。现在一切都在网上进行,A、B 之间可能远隔重洋,怎么办?RSA 的数字签名考虑如下。

S1 A 用他所持有的密码 d_A,计算 $S=m^{d_A}(\bmod n_A)$。

S2 A 将(m,S) 同时寄给 B,B 收到后计算得 $m^*=S^{e_A}(\bmod n_A)$。

若 m^* 和 m 一致,则可确信是 A 发来的,否则予以拒绝。若 A 过后反悔,A 可向执法机关出示(m,S) 作凭证,因为只有 A 才能产生与 m 相对应的 S。因为:

$$S^{e_A}(\bmod n_A)=(m^{d_A}(\bmod n_A))^{e_A}(\bmod n_A)\equiv(m)^{e_Ad_A}(\bmod n_A)\equiv m^{k\phi(n_A)+1}(\bmod n_A)$$
$$\equiv(m^{\phi(n_A)}(\bmod n_A))^k m(\bmod n_A)\equiv m$$

1.16 Karatsuba-Offman 算法及中国剩余定理在解密过程中的应用

(1) 两个 n 位数 A 和 B 的积,通常要作 n^2次一位数的乘法来实现,令 $A=a_1\times 10^{\frac{n}{2}}+a_2$、$B=b_1\times 10^{\frac{n}{2}}+b_2$。令 $P=(a_1+a_2)(b_1+b_2)$、$Q=a_1b_1$、$R=a_2b_2$,则

$$AB=(a_1\times 10^{\frac{n}{2}}+a_2)(b_1\times 10^{\frac{n}{2}}+b_2)=a_1b_110^n+(a_1b_2+a_2b_1)10^{\frac{n}{2}}+a_2b_2$$
$$=Q\cdot 10^n+(P-Q-R)10^{\frac{n}{2}}+R$$

利用以上公式求 AB 不再是作 n^2次一位数的乘法,而是作三次$\frac{n}{2}$ 位数的乘法,加上若干加法及移位。

令 T_n为 $N=2^n$是所作一位数乘法的次数,则

$$T_n=3T_{n-1}\quad T_0=1\quad T_n=3^n$$

另 $N=2^n$，则 $T_n=3^{\log N}$，这里 $\log n$ 以 2 为底。

上述算法可应用于 $2n$ 位二进制数的算法，令 $u=(u_{2n-1}u_{2n-2}\cdots u_1u_0)_2$、$v=(v_{2n-1}v_{2n-2}\cdots v_1v_0)_2$。令 $\overline{u_1}=(u_{2n-1}u_{2n-2}\cdots u_n)_2$、$\overline{u_0}=(u_{n-1}u_{n-2}\cdots u_1u_0)_2$。则

$$\overline{v_1}=(v_{2n-1}v_{2n-2}\cdots v_n)_2 \quad \overline{v_0}=(v_{n-1}v_{n-2}\cdots v_1v_0)_2$$

$$uv=(2^{2n}+2^n)\overline{u_1}\,\overline{v_1}+2^n(\overline{u_1}-u_0)(\overline{v_1}-\overline{v_0})+(2^n+1)\overline{u_0}\,\overline{v_0}$$

可见 uv 可通过三次 n 位二进制数乘法和若干加法和移位来实现。$N=2^n$，同样令 T_n 表示 $N=2^n$ 位二进制数算法所作的一位数乘法次数，则 $T_n=3^{\log_2 N}$。

RSA 加、解密有大量的乘法运算，利用 Karatsuba-Offman 算法可以节省时间。

(2) 中国剩余定理在作大数模、幂运算时可以加快解密速度，RSA 解密时要作大数的模幂运算：

$$m\equiv C^d \pmod n$$

根据 Fermat 定理：$C^{p-1}\equiv 1\pmod n$，令 $m_1\equiv C^d\pmod p\equiv (C\pmod p)^{d(\bmod (p-1))}\pmod p$，$m_2\equiv C^d\pmod q\equiv (C\pmod q)^{d(\bmod (q-1))}\pmod q$。

根据中国剩余定理先求：

$$\begin{cases} qy_1\equiv 1\pmod p \\ py_2\equiv 1\pmod q \end{cases}$$

的解 y_1、y_2，由于解密用户知道 p 和 q，故

$$y_1\equiv q^{-1}\pmod p \quad y_2\equiv p^{-1}\pmod q$$

$(p,q)=1$ 故存在 k 和 h 两整数，使 $1=hp+kq$。

$$h\equiv p^{-1}\pmod q \quad k\equiv q^{-1}\pmod p$$

$$m\equiv kqm_1+hpm_2\pmod n\equiv qy_1m_1+py_2m_2\pmod n$$

若预先储存 kq 和 hp 可以节省许多时间。

1.17　指数和原根

定义 1-5：设 a 和 m 是互素的两个正整数，最小的正整数 x 满足 $a^x\equiv 1\pmod m$，则称 x 为 $a\pmod m$ 的指数。

例 1-20　求 2 对 $(\bmod 7)$ 的指数。

$2^1\equiv 2$、$2^2\equiv 4$、$2^3\equiv 6\pmod 7$，故 2 对 $(\bmod 7)$ 的指数是 3。

同理 $3^1\equiv 3$、$3^2\equiv 2$、$3^3\equiv 6$、$3^4\equiv 4$、$3^5\equiv 5$、$3^6\equiv 1\pmod 7$，故 $3\pmod 7$ 的指数是 6。

定理 1-22：若 a 与 n 互素，$a\pmod n$ 的指数是 δ，$n>0$，正整数 x 使 $a^x\equiv 1\pmod n$，则当且仅当 $\delta|x$ 时成立。

证　若 $\delta|x$，令 $x=k\delta$，k 是正整数。$a^x\equiv a^{k\delta}\equiv (a^k)^\delta\equiv 1\pmod n$，充分性得到了证明。

反之，若 $a^x\equiv 1\pmod n$，令 $x=qx+r$，$0\leqslant r<\delta$，则 $a^x=a^{q\delta+r}=(a^\delta)^q\cdot a^r\equiv a^r\pmod n\equiv 1$，与 $r<\delta$ 的假定矛盾，故 $r=0$，即 $\delta|x$。

推论：若 a 与 n 互素，$n>0$，a 对 mod n 的指数是 δ，则 $\delta|\phi(n)$。

证　因 $(a,n)=1$，根据 Euler 定理 $a^{\phi(n)}\equiv 1\pmod n$，$\delta$ 是使 $a^\delta\equiv 1\pmod n$ 成立的最小整数，所以 $\delta|\phi(n)$。

例 1-21 $\phi(9)=6$，除尽 6 的数有 1、2、3，求 7(mod 9) 的指数。

$7^1\equiv7(\text{mod } 9)$、$7^2\equiv49\equiv4(\text{mod } 9)$、$7^3\equiv343\equiv38\times9+1$、$7^3\equiv1(\text{mod } 9)$，故 7(mod 9) 的指数是 3，$3\mid\phi(9)$。

例 1-22 求 5(mod 17)的指数。

17 是素数，$\phi(17)=16$，除尽 16 的数有 1、2、4、8、16。即

$5^1\equiv5(\text{mod } 17)$，$5^2=25\equiv8(\text{mod } 17)$，$5^4=625\equiv36\times17+13$。故 $5^4\equiv13(\text{mod } 17)$。

$$5^8\equiv390\,625\equiv22\,977\times17+16\equiv16(\text{mod } 17)$$

故 mod 17，5 的指数是 16。

定理 1-23：a 和 n 是互素的整数，$n>0$，$a^i\equiv a^j(\text{mod } n)$，$i$ 和 j 是整数，当且仅当 $i\equiv j(\text{mod } \delta)$，$\delta$ 是 mod n，a 的指数。

证 若 $i\equiv j(\text{mod } \delta)$，假定 $j>i\geqslant0$，$j=k\delta+i$，$a^j\equiv a^{k\delta+i}\equiv a^i(\text{mod } \delta)$，充分性得证。

反之若 $a^i\equiv a^j(\text{mod } n)$，$j\geqslant i$，$(a,n)=1$，所以$(a^i,n)=1$，根据定理，若 $ab\equiv ac(\text{mod } n)$，$(a,n)=1$，则 $b\equiv c(\text{mod } n)$，$a^j=a^{j-i}\cdot a^i\equiv a^i(\text{mod } n)$，即 $a^{j-i}\equiv1(\text{mod } n)$，所以 $\delta\mid j-i$，即 $j\equiv i(\text{mod } \delta)$。

推论：已知$(a,n)=1$，$a^\alpha=1(\text{mod } n)$，$(\alpha,\beta)=d$，则 $a^\alpha(\text{mod } n)$ 的指数是 α/d。

定义 1-6：若 r 与 n 互素，$n>0$，令 mod n r 的指数是 $\phi(n)$，则称 r 是 mod n 的原根。

例如：$\phi(7)=6$，$3^6\equiv1(\text{mod } 7)$，$(3,7)=1$。所以 mod 7，3 的指数是 $\phi(7)$，所以 3 是 mod 7 的原根。5 也是 mod 7 的原根。但并非所有的整数都有原根，8 就可证明没有原根。

在 1～30 的 30 个整数中，2、3、4、5、6、7、9、10、11、13、14、17、18、19、22、23、25、26、27、29 有原根。8、12、15、16、20、21、24、28、30 无原根。

定理 1-24：若 r 是 mod n 的原根，$(r,n)=1$，则 r^1、r^2、…、$r^{\phi(n)}$ 形成 mod n 的简化剩余解。

证 只要证 r^1、r^2、…、$r^{\phi(n)}(\text{mod } n)$两两不同余。如若不然，$r^i\equiv r^j(\text{mod } n)$。假定 $\phi(n)>1$，$j>i$，则有 $r^{j-i}\equiv1(\text{mod } n)$。

$j-i<\phi(n)$，与 r 是(mod n)的原根的假定相矛盾。

这就说明 r^1、r^2、…、$r^{\phi(n)}(\text{mod } n)$两两不同余。

定理 1-25：设 δ 是 $a(\text{mod } n)$的指数，n 是一正整数，则 a^u 的指数为 s，有 $s=\delta/(\delta,u)$。

证 令 $v=(\delta,u)$，$\delta=t_1v$，$u=u_1v$，$(t_1,u_1)=1$。

$$(a^u)^{t_1}=(a^{u_1v})^{(\delta/v)}=(a^\delta)^{u_1}\equiv1(\text{mod } n)$$

所以 $s\mid t_1$。

另外$(a^u)^s\equiv1(\text{mod } n)$，所以 $\delta\mid us$，$t_1v\mid u_1vs$，$t_1\mid u_1s$。

因$(t_1,u_1)=1$，所以 $t_1\mid s$，$t_1=s=\dfrac{t}{(\delta,u)}$。 证毕

例 1-23 mod 7，3 的指数是 6，mod 7，3^4 的指数$=\dfrac{6}{(6,4)}=3$。

推论：r 是 mod n 的原根，$n>1$，则 r^u是 mod n 的原根当且仅当$(u,\phi(n))=1$ 时成立。

由定理知 mod n r^u的指数 s 有：

$$s=\frac{\delta}{(u,\delta)}=\frac{\phi(n)}{(u,\phi(n))}$$

所以 mod n，r^u 是原根的充要条件是$(u,\phi(n))=1$。

上面已经交代过并不是所有整数都有原根。总之，模 2、4、p^α、$2p^\alpha(\alpha\geqslant1)$，$p$ 是素数有原根，仅这些整数有原根，对应素数 $p<1000$ 的原根列表可参阅一般数论书籍。

1.18　指标（离散对数）

定义 1-7：设 a 是一整数$(a,n)=1$，对模 n 的一个原根 r，有一整数 β 使 $a\equiv r^\beta(\mathrm{mod}\ n)$，$\beta\geqslant0$，则称 β 为以 r 为底 mod n 的指标，记 $\beta=\mathrm{ind}_r a$。

已知 a 求 β，使 $a\equiv r^\beta(\mathrm{mod}\ n)$称为解"离散对数"问题。已知$(a,n)=1$，$r$ 是 mod n 的原根，指标不仅与模有关，而且与原根也有关，之所以省去 mod n，只写 $\mathrm{ind}_r a=\beta$，那是因为 mod n 是固定的。

例 1-24　$m=7$，3 是 mod 7 的原根，所以 mod 7 有 $\mathrm{ind}_3 1=6$，$\mathrm{ind}_3 2=2$，$\mathrm{ind}_3 3=1$，$\mathrm{ind}_3 4=4$，$\mathrm{ind}_3 5=5$，$\mathrm{ind}_3 6=3$。

5 也是 mod 7 的原根，故有 $\mathrm{ind}_5 1=1$、$\mathrm{ind}_5 2=4$、$\mathrm{ind}_5 3=5$、$\mathrm{ind}_5 4=2$、$\mathrm{ind}_5 5=1$、$\mathrm{ind}_5 6=3$。

定理 1-26：令 m 是一正整数有原根 r，a、b 和 m 互素，则有以下结论。

（1）$\mathrm{ind}_r 1=0(\mathrm{mod}\ \phi(m))$。

（2）$\mathrm{ind}_r(a\cdot b)\equiv\mathrm{ind}_r a+\mathrm{ind}_r b(\mathrm{mod}\ \phi(m))$。

（3）$\mathrm{ind}_r a^k\equiv k\cdot\mathrm{ind}_r a(\mathrm{mod}\ \phi(m))$，$k$ 是一正整数。

证　（1）由 Euler 定理 $r^{\phi(m)}\equiv1(\mathrm{mod}\ m)$，$r$ 是 mod m 的一个原根，没有比 r 更少的正次方同余 1(mod m)，所以 $\mathrm{ind}_r 1=\phi(m)(\mathrm{mod}\ \phi(m))$。

（2）根据定义：

$$r^{\mathrm{ind}_r(ab)}\equiv ab(\mathrm{mod}\ m)$$

$$r^{\mathrm{ind}_r a+\mathrm{ind}_r b}\equiv r^{\mathrm{ind}_r a}+r^{\mathrm{ind}_r b}\equiv ab(\mathrm{mod}\ m)$$

所以 $r^{\mathrm{ind}_r(ab)}\equiv r^{\mathrm{ind}_r a+\mathrm{ind}_r b}(\mathrm{mod}\ m)$，$\mathrm{ind}_r(ab)\equiv\mathrm{ind}_r a+\mathrm{ind}_r b(\mathrm{mod}\ \phi(m))$。

因为若 a 和 n 互素，$n>0$，$a^i\equiv a^j(\mathrm{mod}\ n)(i,j\geqslant0)$，则当且仅当 $i\equiv j(\mathrm{mod}\ \delta)$时，$\delta$ 是 a mod n 的指数，即使 $a^x\equiv1(\mathrm{mod}\ n)$成立的最小数 x，由$(a,n)=1$，所以 $\delta=\phi(n)$。

（3）根据定义：

$$r^{\mathrm{ind}_r a^{(ab)}}\equiv ab(\mathrm{mod}\ n)$$

$$r^{k\mathrm{ind}_r a}\equiv(r^{\mathrm{ind}_r a})\equiv ab(\mathrm{mod}\ n)$$

所以 $r^{\mathrm{ind}_r a^{(ab)}}\equiv r^{k\mathrm{ind}_r a}(\mathrm{mod}\ n)$，故 $\mathrm{ind}_r a^k\equiv k\cdot\mathrm{ind}_r a(\mathrm{mod}\ n)$。

例 1-25　已知 mod 7，$\mathrm{ind}_5 2=4$，$\mathrm{ind}_5 3=5$，$\phi(7)=6$，故 $\mathrm{ind}_5 6=\mathrm{ind}_5(2\times3)=\mathrm{ind}_5 2+\mathrm{ind}_5 3=4+5\equiv3(\mathrm{mod}\ 6)$，$\mathrm{ind}_5 3^4=4\mathrm{ind}_5 3=4\times5\equiv20\equiv2(\mathrm{mod}\ 6)$。

或 $\mathrm{ind}_5 3^4=\mathrm{ind}_5 81=\mathrm{ind}_5 4\equiv2$ (mod 7)，$\mathrm{ind}_5 3^4\equiv81\equiv4(\mathrm{mod}\ 7)$，$x\equiv2(\mathrm{mod}\ 6)$，故 $\mathrm{ind}_5 81=2$。

例 1-26　$n=17$，$\phi(17)=16$，求满足 $6x^{12}\equiv11(\mathrm{mod}\ 17)$ 的 x。

解：$3^1\equiv3$，$3^2\equiv9$，$3^3\equiv10$，$3^4\equiv13$，$3^5\equiv5$，$3^6\equiv15$，$3^7\equiv11$，$3^8\equiv16$

$$3^9 \equiv 14, 3^{10} \equiv 8, 3^{11} \equiv 7, 3^{12} \equiv 4, 3^{13} \equiv 12, 3^{14} \equiv 2, 3^{15} \equiv 6, 3^{16} \equiv 1 \pmod{17}$$

故

$$\mathrm{ind}_3 1 = 16 \quad \mathrm{ind}_3 2 = 14 \quad \mathrm{ind}_3 3 = 1 \quad \mathrm{ind}_3 4 = 12 \quad \mathrm{ind}_3 5 = 5 \quad \mathrm{ind}_3 6 = 15$$
$$\mathrm{ind}_3 7 = 11 \quad \mathrm{ind}_3 8 = 10 \quad \mathrm{ind}_3 9 = 2 \quad \mathrm{ind}_3 10 = 3 \quad \mathrm{ind}_3 11 = 7 \quad \mathrm{ind}_3 12 = 13$$
$$\mathrm{ind}_3 13 = 4 \quad \mathrm{ind}_3 14 = 9 \quad \mathrm{ind}_3 15 = 6 \quad \mathrm{ind}_3 16 = 8$$

对 $6x^{12} \equiv 11 \pmod{17}$进行 ind_3的运算得

$$\mathrm{ind}_3(6x^{12}) \equiv \mathrm{ind}_3 6 + \mathrm{ind}_3 x^{12} \equiv 15 + 12\mathrm{ind}_3 x \pmod{17}$$
$$15 + 12\mathrm{ind}_3 x = \mathrm{ind}_3 11 = 7 \quad 12\mathrm{ind}_3 x = 8$$

根据公式,若 $ac \equiv bc \pmod{m}$,$(c,m)=d$,则 $a \equiv b\left(\bmod \dfrac{m}{d}\right)$。

$$3\mathrm{ind}_3 x = 2 \pmod{4}$$
$$\mathrm{ind}_3 x \equiv 2、6、10、14、\pmod{16}$$
$$x = 3^2、3^6、3^{10}、3^{14}、\pmod{17}$$
$$\mathrm{ind}_3 x \equiv 9、15、8、2 \pmod{17}$$

例 1-27 试验证 mod 41 有原根 6,mod 41 有:

$$6^0 \equiv 1 \quad 6^1 \equiv 6 \quad 6^2 \equiv 36 \quad 6^3 \equiv 11 \quad 6^4 \equiv 25 \quad 6^5 \equiv 27 \quad 6^6 \equiv 39 \quad 6^7 \equiv 29 \quad 6^8 \equiv 10$$
$$6^9 \equiv 19 \quad 6^{10} \equiv 32 \quad 6^{11} \equiv 28 \quad 6^{12} \equiv 4 \quad 6^{13} \equiv 24 \quad 6^{14} \equiv 21 \quad 6^{15} \equiv 3 \quad 6^{16} \equiv 18$$
$$6^{17} \equiv 26 \quad 6^{18} \equiv 33 \quad 6^{19} \equiv 34 \quad 6^{20} \equiv 40 \quad 6^{21} \equiv 35 \quad 6^{22} \equiv 5 \quad 6^{23} \equiv 30 \quad 6^{24} \equiv 16$$
$$6^{25} \equiv 14 \quad 6^{26} \equiv 2 \quad 6^{27} \equiv 12 \quad 6^{28} \equiv 31 \quad 6^{29} \equiv 23 \quad 6^{30} \equiv 10 \quad 6^{31} \equiv 13 \quad 6^{32} \equiv 37$$
$$6^{33} \equiv 17 \quad 6^{34} \equiv 20 \quad 6^{35} \equiv 38 \quad 6^{36} \equiv 23 \quad 6^{37} \equiv 15 \quad 6^{38} \equiv 8 \quad 6^{39} \equiv 7 \quad 6^{40} \equiv 1$$

故得 mod 41 有:

$$\mathrm{ind}_6 1 = 0 \quad \mathrm{ind}_6 2 = 26 \quad \mathrm{ind}_6 3 = 15 \quad \mathrm{ind}_6 4 = 12 \quad \mathrm{ind}_6 5 = 22$$
$$\mathrm{ind}_6 6 = 1 \quad \mathrm{ind}_6 7 = 39 \quad \mathrm{ind}_6 8 = 38 \quad \mathrm{ind}_6 9 = 30 \quad \mathrm{ind}_6 10 = 8$$
$$\mathrm{ind}_6 11 = 3 \quad \mathrm{ind}_6 12 = 27 \quad \mathrm{ind}_6 13 = 31 \quad \mathrm{ind}_6 14 = 25 \quad \mathrm{ind}_6 15 = 37$$
$$\mathrm{ind}_6 16 = 24 \quad \mathrm{ind}_6 17 = 33 \quad \mathrm{ind}_6 18 = 16 \quad \mathrm{ind}_6 19 = 9 \quad \mathrm{ind}_6 20 = 34$$
$$\mathrm{ind}_6 21 = 14 \quad \mathrm{ind}_6 22 = 29 \quad \mathrm{ind}_6 23 = 36 \quad \mathrm{ind}_6 24 = 13 \quad \mathrm{ind}_6 25 = 4$$
$$\mathrm{ind}_6 26 = 17 \quad \mathrm{ind}_6 27 = 5 \quad \mathrm{ind}_6 28 = 11 \quad \mathrm{ind}_6 29 = 7 \quad \mathrm{ind}_6 30 = 23$$
$$\mathrm{ind}_6 31 = 28 \quad \mathrm{ind}_6 32 = 10 \quad \mathrm{ind}_6 33 = 18 \quad \mathrm{ind}_6 34 = 19 \quad \mathrm{ind}_6 35 = 21$$
$$\mathrm{ind}_6 36 = 2 \quad \mathrm{ind}_6 37 = 22 \quad \mathrm{ind}_6 38 = 35 \quad \mathrm{ind}_6 39 = 6 \quad \mathrm{ind}_6 40 = 20$$

1.19 Miller 素数判定法

公钥密码 RSA 要求大量的大素数 p 和 q,大到至少 1024 位,所以如何判定大素数成为数论研究中的重要问题。前面涉及素数的有 Wilson 定理和 Fermat 定理。Wilson 是判定素数的充要条件:$(p-1)! \equiv 1 \pmod{p}$,但用来判定大素数几乎是做不到的。Fermat 给出 p 是素数的必要条件:$a^{p-1} \equiv 1 \pmod{p}$,可以作为非素数的判定。

Miller 判定法:n 为一正整数且 $n \nmid b$,$n-1=2^s t$,s 为非负整数,t 是奇整数,若 $b^t \equiv 1 \pmod{n}$,或 $b^{2^j t} \equiv -1 \pmod{n}$ $(0 \leqslant j \leqslant s-1)$,则称 n 通过以 b 为基的 Miller 测试。

定理 1-27：若 n 是素数，且 $n\nmid b$，则 n 通过以 b 为基的 Miller 测试。

证　令 $\xi_k=b^{\frac{n-1}{2^k}}=b^{2^{s-k}t}(k=s,s-1,\cdots,1,0)$。因 n 是素数，$\xi_0=b^{n-1}\equiv1(\mathrm{mod}\ n)$(Fermat 定理)。它的必然结果是 $\xi_1\equiv b^{\frac{n-1}{2}}\equiv1(\mathrm{mod}\ n)$，或 $\xi_1\equiv b^{\frac{n-1}{2}}\equiv-1(\mathrm{mod}\ n)$。

因 $\xi_0\equiv\xi_1^2(\mathrm{mod}\ n)$，Fermat 定理成立。

同理 $\xi_2\equiv1(\mathrm{mod}\ n)$，或 $\xi_2\equiv-1(\mathrm{mod}\ n)$ 成立，则 $\xi_1\equiv1(\mathrm{mod}\ n)$。

满足 Fermat 定理，以此类推，若已知 $\xi_{k+1}\equiv1(\mathrm{mod}\ n)$，或 $\xi_{k+1}\equiv-1(\mathrm{mod}\ n)$，则 $\xi_k\equiv\xi_{k-1}\equiv\cdots\equiv\xi_0\equiv1(\mathrm{mod}\ n)$。说明一旦 Miller 测试通过，Fermat 定理便获得满足。

注意：计算 ξ_k 的过程是 $k=s,s-1,\cdots,1,0$。

定理 1-28：若 n 是正奇数，则 n 通过以 b 为基的 Miller 测试至多是$\frac{1}{4}(n-1)$。

定理是非常明白的，证明从略。

已知 $n-1=2^st$，Miller 测试的步骤如下。

S1 在$\{1,2,\cdots,n-1\}$中随机地产生一个数 b，$j\leftarrow0$，计算 $z\leftarrow b^t(\mathrm{mod}\ n)$；

S2 若 $z=1$ 则转 S7；

S3 $i\leftarrow1$；

S4 若 $z=n-1$ 则转 S7；

S5 若 $i=s$，则 n 非素数，结束，否则转 S6；

S6 $z\leftarrow z^2(\mathrm{mod}\ n)$，若 $i\leftarrow i+1$ 转 S4；

S7 n 通过 Miller 测试。

可见若 n 是合数，n 通过 Miller 测试的概率小于$\frac{1}{4}$。

定理 1-29：令 n 是正整数，取 k 个 b，使 n 通过 Miller 测试，n 是合数，通过 k 次 Miller 测试的概率小于$\left(\frac{1}{4}\right)^k$。

令 n 是一合数，随机取 100 个不同的整数作为基，n 通过所有的 Miller 测试的概率小于$\left(\frac{1}{4}\right)^{100}\approx6.22\times10^{-61}<10^{-60}$。

尽管 n 是合数，但能通过 100 次 Miller 测试，出错的概率小于 10^{-6}，应该说基本上是不可能的小概率事件，但毕竟是小概率事件，能不能有确定的算法判定素数呢，答案是肯定的。近来(2002 年)有 AKS 算法脱颖而出，而且是多项式型算法。但 AKS 算法还需要其他数学分支的支持，在此从略。

1.20　ElGamal 公钥密码

ElGamal 公钥密码是几乎和 RSA 同时出现的公钥密码，如果说 RSA 公钥的破译困难是基于大数的分解困难，对 ElGamal 的攻击的困难则在于求解离散对数的难度，到现在为止，还没谈及求离散对数的方法。

1. ElGamal 的加密算法

设有一大素数 p 及 mod p 的原根 g。每一个用户(设为 A)选择一整数 x_A,$0\leqslant x_A\leqslant p-1$,计算 $y_A\equiv g^{x_A}(\bmod p)$。

将 y_A公开,x_A由 A 自己保密掌握。

S1 若 A 将信息 m 秘密送到 B,A 找到 $y_B\equiv g^{x_B}(\bmod p)$。

S2 A 随机地选一整数 x,$0\leqslant x\leqslant p-1$,计算 $C_1\equiv g^x(\bmod p)$。

S3 A 计算 $K\equiv(g_B)^x\equiv g^{xx_B}(\bmod p)$。

计算 $C_2\equiv Km(\bmod p)$。

S4 A 将(C_1,C_2)作密文寄给 B。

B 收到(C_1,C_2)后,解密如下。

S1 B 利用他保密掌握的 x_B,计算$(C_1)^{x_B}\equiv(g^x)^{x_B}\equiv(y_B)^x(\bmod p)\equiv K$。

S2 B 计算 $K^{-1}(\bmod p)$。

S3 $m\equiv K^{-1}C_2(\bmod p)$。

任一第三者无法从 C_1求得 x,也无法从公开的 y_B求得 k 及 $K^{-1}(\bmod p)$。

例 1-28 设 $p=11$,mod 11 的原根 $g=7$,设 $x_A=3$,$y_A\equiv 7^3\equiv 343(\bmod 11)\equiv 2$;设 $x_B=5$,$y_B\equiv 7^5\equiv 16\,807(\bmod 11)\equiv 10$;设 $m=6$,A 取 $x=7$。

$$C_1\equiv 7^7(\bmod 11)\equiv 490(\bmod 11)\equiv 6$$
$$K\equiv(10)^7(\bmod 11)\equiv 10$$
$$C_2\equiv 10\times 6(\bmod 11)\equiv 5$$

A 将(C_1,C_2)寄给 B,B 收到(C_1,C_2)后解密如下:

$$K\equiv(g)^5\equiv(7^5)(\bmod 11)\equiv 10$$
$$K^{-1}\equiv(7)^{10-5}(\bmod 11)\equiv 10$$
$$m\equiv K^{-1}C_2\equiv 50(\bmod 11)\equiv 6$$

2. ElGamal 的数字签名

设有一大素数 p 及 mod p 的原根 g,S1 发信方 A 选一整数 S,$0\leqslant S\leqslant p-1$,要求 $(S,p-1)=1$。

S2 计算 $W\equiv g^S(\bmod p)$,令 $m=x_AW+SV(\bmod p-1)$,解出 V,A 将(W,V)作为 m 的数字签名,将(m,W,V)寄给 B。

$$g^m\equiv g^{x_AW+SV}\equiv(g^{x_A})^W(g^x)^V(\bmod p)(y_A)^WW^V(\bmod p)$$

例 1-29 $p=11$,mod 11 的原根 $g=7$,$x_A=3$,$y_A\equiv 7^3(\bmod 11)=2$,若 $m=6$,A 取 $S=7$,满足$(S,p-1)=(7,10)=1$,$W\equiv 7^7(\bmod 11)\equiv 6$,$m=x_AW+SV(\bmod 10)$,即 $6\equiv 3\times 6+7V(\bmod 10)$,$7V\equiv -12\equiv 8(\bmod 10)$,$V\equiv 7^{-1}\times 8\equiv 3\times 8(\bmod 10)\equiv 4$,故密文是(6,6,4)。

收信方收到密文后,验证如下:

$$(y_A)^W\cdot W^V\equiv(2)^6\times 6^4\equiv 82\,944(\bmod 11)\equiv 4$$

$$(g)^m(\bmod\ p) \equiv (7)^6(\bmod\ 11) \equiv 4$$
$$(g^m) \equiv (y_A)^W \cdot W^V(\bmod\ 11)$$

故予以接受。

例 1-30　设 m=public key cryptography。

将 m 分组如下：

pu bl ic ke yc ry pt og ra ph yx

x 是补上的空格，按 a 为 00，b 为 01，…，x 为 23，y 为 24，得

1520 0111 0804 1004 2402 1724 1519 1406 1700 1507 2423

以第一组为例

$$m = 1520,\quad p = 2539,\quad g = 2,\quad x_A = 14,$$
$$y_A \equiv 2^{14}(\bmod\ 2539) \equiv 16\ 384(\bmod\ 2539) \equiv 1150$$

向 A 发送 m，取 S=1443，

$$(S,p-1) = (1443,2538) = (1443,1095) = (384,1095) = (384,327)$$
$$= (57,327) = (57,42) = (13,42) = (13,3) = 1$$

$$C_1 \equiv 2^{1443}(\bmod\ 2539) \equiv 2141$$
$$K \equiv (1150)^{1443}(\bmod\ 2539)$$
$$C_2 \equiv 1520 \times 1150^{1443}(\bmod\ 2539) \equiv 216$$

$C = (2141,216)$，送 A。

A 收到后解密得

$$m \equiv (2141)^{-14} \cdot 0216(\bmod\ 2539) \equiv 2452 \cdot 0216 \bmod (2539)$$
$$\equiv 529\ 632(\bmod\ 2539) \equiv 1520$$

明文被分成 11 组，第一组加密如上所述，其实每一组可采用不同的 S，使破译更加困难。

以后各节一律作为自由选读，本章不再说明。

1.21　平方剩余与非平方剩余，Legender 符号

定义 1-8　m 是正整数，$(a,m)=1$，若 $x^2\equiv a(\bmod\ m)$ 有解，则称 a 是 mod m 的平方剩余，若 $x^2\equiv a(\bmod\ m)$ 无解，则称 a 为 mod m 的非平方剩余。

例 1-31　mod 11，$1^2\equiv1$，$2^2\equiv4$，$3^2\equiv4$，$4^2\equiv5$，$5^2\equiv3$，$6^2\equiv3$，$7^2\equiv5$，$8^2\equiv9$，$9^2\equiv4$，$10^2\equiv1$。所以 1、3、4、5、9 是 mod 11 的平方剩余，2、6、7、8、10 是 mod 11 的非平方剩余。

引理：设 p 是一奇素数，a 不是 p 的倍数，则 $x^2\equiv a(\bmod\ p)$ 或有两个 mod p 不同余的解，或无解。

证　若 $x^2\equiv a(\bmod\ p)$ 有一解 x_0，立即可得 $x=-x_0(\bmod\ p)$ 是另一个 mod p 不同余的解，$(-x_0)^2=x_0^2\equiv a(\bmod\ p)$ $-x_0\not\equiv x_0(\bmod\ p)$，否则 $2x_0\equiv0(\bmod\ p)$，因 p 是奇素数，故这是不可能的，$p\nmid x_0$。

不会有另外的两个不同余解，如若不然，$x=x_0$ 和 $x=x_1$ 都满足 $x^2\equiv a(\bmod\ p)$，$x_0^2\equiv x_1^2\equiv a(\bmod\ p)$，$x_0^2-x_1^2=(x_0-x_1)(x_0+x_1)$，故 $(x_0-x_1)(x_0+x_1)\equiv0(\bmod\ p)$，则 $p\mid(x_0+x_1)$ 或 $p\mid(x_0-x_1)$，即 $x_1\equiv-x_0(\bmod\ p)$，$x_1\equiv x_0(\bmod\ p)$，所以 $x^2\equiv a(\bmod\ p)$ 有一解，则有

两个不同余的解。

定理 1-30：p 是奇素数，则在$[1,2,\cdots,p-1]$中 mod p 有$\frac{1}{2}(p-1)$个平方剩余，$\frac{1}{2}(p-1)$个非平方剩余。

证 (1) 若 $x^2\equiv a(\bmod p)$ 有解，其解必定只能在下面 $p-1$ 个数之中：$\pm 1,\pm 2,\cdots,\pm\frac{p-1}{2}$。

因$(a,p)=1$，即 $p\nmid a$，而这 $p-1$ 个数的平方只能是下面$\frac{1}{2}(p-1)$ 个数：$1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$，所以 mod p 的平方剩余最多有$\frac{1}{2}(p-1)$ 个。

(2) $1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$ 这$\frac{1}{2}(p-1)$个数中不存在两个是 mod p 同余的。

如若不然，有

$$1\leqslant l<k\leqslant\frac{p-1}{2},\quad 使\ l^2\equiv k^2(\bmod p)$$

$$(k-l)(k+l)\equiv 0(\bmod p)$$

$$1<k+l<p-1,\quad 1\leqslant k-l<\frac{p-1}{2}$$

因此 $l^2\equiv k^2(\bmod p)$是不可能成立的，从而 $l^2\not\equiv k^2(\bmod p)$，这说明 $1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$ 都是 mod p 的平方剩余。

(3) 在$(a,p)=1$，即 $p\nmid a$ 的 $p-1$ 个数 a，p 是素数，p 与 a 互素而且 $a<p$，则显然 a 的数目为 $p-1$。

$1,2,\cdots,p-1$，或在$\pm 1,\pm 2,\cdots,\pm\frac{1}{2}(p-1)$之中，除去$\frac{1}{2}(p-1)$个平方剩余，其余的$\frac{1}{2}(p-1)$个显然就是 mod p 的非平方剩余了。

定理 1-31：(Euler 的判别条件)：

若 a 是 mod p 的平方剩余，则 $a^{\frac{p-1}{2}}\equiv 1(\bmod p)$。

若 b 是 mod p 的非平方剩余，则 $b^{\frac{p-1}{2}}\equiv -1(\bmod p)$。

证 $x^2\equiv a(\bmod p)$ 有解 r，$1\leqslant r\leqslant p-1$，根据 Euler 定理 $r^{\phi(p)}\equiv r^{p-1}\equiv 1(\bmod p)$，即 $a^{\frac{1}{2}(p-1)}\equiv(r^2)^{\frac{1}{2}(p-1)}\equiv r^{p-1}\equiv 1(\bmod p)$，$x^{p-1}\equiv 1(\bmod p)$ 有 $p-1$ 个解：$1,2,\cdots,p-1$，或 $(x^{\frac{p-1}{2}}-1)(x^{\frac{p-1}{2}}+1)\equiv 0(\bmod p)$，$x^{\frac{p-1}{2}}\equiv 1$ 和 $x^{\frac{p-1}{2}}\equiv -1(\bmod p)$，各有$\frac{1}{2}(p-1)$个解。

a 是 mod p 的平方剩余，则 $a^{\frac{1}{2}(p-1)}\equiv 1(\bmod p)$，其余的$\frac{1}{2}(p-1)$个 mod p 非平方剩余，满足 $b^{\frac{1}{2}(p-1)}\equiv -1(\bmod p)$。

定义 1-9：令 p 为奇素数，a 是整数，$p\nmid a$，Legender 符号$\left(\frac{a}{p}\right)$

$$\left(\frac{a}{p}\right)=\begin{cases}1, & 若 a 是 p 的平方剩余\\ 0, & p \mid a\\ -1, & 若 a 是 \bmod p 的非平方剩余\end{cases}$$

由 Euler 定理，有

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod p$$

定理 1-32：若 $a_1 \equiv a_2 \pmod p$，则 $\left(\frac{a_1}{p}\right)=\left(\frac{a_2}{p}\right)$。

证　因

$$\left(\frac{a_1}{p}\right) \equiv a_1^{\frac{1}{2}(p-1)} \equiv a_2^{\frac{1}{2}(p-1)} \equiv \left(\frac{a_2}{p}\right) \pmod p$$

即

$$\left(\frac{a_1}{p}\right)-\left(\frac{a_2}{p}\right) \equiv 0 \pmod p$$

但 $\left|\left(\frac{a_1}{p}\right)-\left(\frac{a_2}{p}\right)\right| \leqslant 2$，$p$ 是奇素数，$p>2$，所以只能 $\left(\frac{a_1}{p}\right)=\left(\frac{a_2}{p}\right)=0$。

定理 1-33：$\left(\frac{a_1 a_2 \cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$。

证　$\left(\frac{a_1 a_2 \cdots a_n}{p}\right) \equiv (a_1 a_2 \cdots a_n)^{\frac{1}{2}(p-1)} \equiv \prod_{i=1}^{n} a_i^{\frac{1}{2}(p-1)} \equiv \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right) \pmod p$，与上一定理类似地证明：

$$\left(\frac{a_1 a_2 \cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$$

推论 1：$\left(\frac{b^2 c}{p}\right)=\left(\frac{c}{p}\right)$，因 $p \nmid b^2$，所以 $\left(\frac{b^2}{p}\right)=1$。

推论 2：若 $p=4n+1$，则 -1 是 p 的平方剩余；若 $p=4n+3$，则 -1 是 p 的非平方剩余，即

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{1}{2}(p-1)}$$

证　$\left(\frac{-1}{p}\right)=(-1)^{\frac{1}{2}(p-1)} \pmod p$，等式两端只能同时为 1 或同时为 -1，否则 $p \mid 2$，与 p 是奇素数的假定矛盾，故 $\left(\frac{-1}{p}\right)=(-1)^{\frac{1}{2}(p-1)}$，即

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & p \equiv 1 \pmod 4\\ -1, & p \equiv -1 \pmod 4\end{cases}$$

1.22　互倒定理

Gauss 引理　设 $p>2$，$(q,p)=1$，$0<r_1<r_2<\cdots<r_{\frac{p-1}{2}}<p$。

为 $\bmod p$ 的 $\frac{p-1}{2}$ 类不同的剩余

$$q, 2q, \cdots, \frac{p-1}{2}$$

的最小正剩余，若 $r_i, i=1,2,\cdots,\frac{p-1}{2}q$ 中有 μ 个数大于 $\frac{1}{2}p$，则 $\left(\frac{q}{p}\right)=(-1)^{\mu}$。

证　令 $n=\frac{p-1}{2}-\mu$，则 $r_{n+1}, r_{n+2}, \cdots, r_{n+\mu}$ 都大于 $\frac{1}{2}p$，故 $p-r_{n+1}, p-r_{n+2}, \cdots, p-r_{n+\mu}$ 都小于 $\frac{1}{2}p$。

下面证 $\frac{p-1}{2}$ 个数

$$r_1, r_2, \cdots, r_n, p-r_{n+1}, \cdots, p-r_{n+\mu}$$

mod p 两两互不同余，显然

$$r_i \not\equiv r_j \pmod p,\quad 1 \leqslant i < j \leqslant n$$

并且 $(p-r_{n+i}) \not\equiv (p-r_{n+j}) \pmod p, 1 \leqslant i < j \leqslant \mu$。

所以只需证明 $r_k \not\equiv (p-r_\lambda) \pmod p$，则 $r_k+r_\lambda \equiv 0 \pmod p$，而 $r_k \equiv sq, r_\lambda \equiv tq \pmod p$，从而 $(s+t)q \equiv 0 \pmod p$。

但 $(p,q)=1$，故 $s+t \equiv 0 \pmod p$，又因 $0<s,t<\frac{1}{2}p$，故 $s+t \equiv 0 \pmod p$ 不能成立 $r_k \not\equiv (p-r_\lambda) \pmod p$，因此 $r_1, r_2, \cdots, r_n, p-r_{n+1}, \cdots, p-r_{n+\mu}$ 这 $\frac{p-1}{2}$ 个数就是 $1,2,\cdots,\frac{p-1}{2}$ 这 $\frac{p-1}{2}$ 个数，所以

$$1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} \equiv r_1 r_2 \cdots r_n (p-r_{n+1}) \cdots (p-r_{n+\mu}) \equiv (-1)^{\mu} r_1 r_2 \cdots r_{\frac{p-1}{2}} \pmod p$$

将其代入下式

$$1 \cdot 2 \cdots \frac{p-1}{2} \cdot q^{\frac{p-1}{2}} \equiv r_1 r_2 \cdots r_{\frac{p-1}{2}} \pmod p$$

得

$$(-1)^{\mu} r_1 r_2 \cdots r_{\frac{p-1}{2}} q^{\frac{p-1}{2}} \equiv r_1 r_2 \cdots r_{\frac{p-1}{2}} \pmod p$$

故有

$$(-1)^{\mu} q^{\frac{p-1}{2}} \equiv 1 \pmod p$$

即得

$$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod p$$

因 $p>2$，故 $\left(\frac{q}{p}\right)=(-1)^{\mu}$。

定理 1-34：若 $p=8n+1$，则 2 为 p 的平方剩余；若 $p=8n+3$，则 2 为 p 的非平方剩余，即

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

证　用 2 分别乘 $1,2,\cdots,\frac{p-1}{2}$，得 $2,4,\cdots,p-1$，这是 $2r$ 数，若 $2r>\frac{1}{2}p$，即 $r>\frac{1}{4}p$，所以其中大于 $\frac{1}{2}p$ 的数共有

$$\mu=\frac{p-1}{2}-\left\lfloor\frac{p}{4}\right\rfloor$$

若 $p=8n+1$，则 $\mu=4n-2n=2n$。

若 $p=8n+7$，则 $\mu=4n+3-(2n+1)=2n+2$。

若 $p=8n+3$，则 $\mu=4n+1-2n=2n+1$。

若 $p=8n+5$，则 $\mu=4n+2-(2n+1)=2n+1$。

即当 $p=8n\pm1$ 时 μ 为偶数，2 为 p 的平方剩余；当 $p=8n\pm3$ 时 μ 为奇数，2 为 p 的平方非剩余。

又因若 $p=8n\pm1$ 时，则 $\frac{1}{8}(p^2-1)\equiv 8n\pm2n\equiv0 \pmod 2$，$p=8n\pm3$ 时，则 $\frac{1}{8}(p^2-1)\equiv 8n+2n+1\equiv1 \pmod 2$，所以 $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$。

定理 1-35（互倒定理）：若 p 和 q 是两个不同的奇素数，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$$

证　令 $p'=\frac{p-1}{2}$，$q'=\frac{q-1}{2}$，若 mod p，则

$$q,2q,\cdots,p'q$$

代表 p' 表不同的剩余，设

$$q=\left\lfloor\frac{q}{p}\right\rfloor p+r_1$$

$$2q=\left\lfloor\frac{2q}{p}\right\rfloor p+r_2$$

$$\cdots$$

$$p'q=\left\lfloor\frac{p'q}{p}\right\rfloor p+r_p$$

这里 $0<r_i<p'$，$i=1,2,\cdots,p'$，设这 p' 个数 $r_1,r_2,\cdots,r_{p'}$ 中有 n 个小于 $\frac{1}{2}p$，有 μ 个大于 $\frac{1}{2}p$，它们分别是 $a_1,a_2,\cdots,a_n$ 和 $b_1,b_2,\cdots,b_\mu$

$$\sum_{h=1}^{p'}hq=\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor p+\sum_{i=1}^{n}a_i+\sum_{j=1}^{\mu}b_j$$

又由 Gauss 引理的证明知

$$\sum_{h=1}^{p'}h=\sum_{i=1}^{n}a_i+\sum_{j=1}^{\mu}(p-b_j)=\mu p+\sum_{i=1}^{n}a_i-\sum_{j=1}^{\mu}b_j$$

$$\sum_{h=1}^{p'}h=\frac{1}{2}\cdot\frac{p-1}{2}\left(1+\frac{p-1}{2}\right)=\frac{1}{8}(p^2-1)$$

故得

$$\frac{1}{8}(p^2-1)=\mu p+\sum_{i=1}^{n}a_i-\sum_{j=1}^{\mu}b_j$$

由前面两等式得

$$\frac{p^2-1}{8}(q-1)=\sum_{h=1}^{n'}\left\lfloor\frac{hq}{p}\right\rfloor p-\mu p+2\sum_{j=1}^{\mu}b_j$$

故有

$$\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor p\equiv\mu p\pmod 2$$

即

$$\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor\equiv\mu\pmod 2$$

由 Gauss 引理可得 $\left(\frac{q}{p}\right)=(-1)^{\mu}=(-1)^{\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor}$。

同理可得 $\left(\frac{p}{q}\right)=(-1)^{\sum_{k=1}^{q'}\left\lfloor\frac{kp}{q}\right\rfloor}$。

下面证

$$\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor+\sum_{k=1}^{q'}\left\lfloor\frac{kp}{q}\right\rfloor=\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$$

注意形如$\frac{h}{p}-\frac{k}{q}$的数，其中 $h=1,2,\cdots,p'$;$k=1,2,\cdots,q'$。

共有 $p'q'=\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ 个，它们全不为零，因若$\frac{h}{p}-\frac{k}{q}=0$，则 $hq=ky$，因而 $p\nmid q,0<h<p'=\frac{1}{2}(p-1)$，上式不可能成立。

再看$\frac{h}{p}-\frac{k}{q}$ 有多少为正和多少为负的。

先看$\frac{h}{p}-\frac{k}{q}>0$，即 $k<\frac{hq}{p}$，故当 h 确定时共有$\left\lfloor\frac{hq}{p}\right\rfloor$个 k，所以共有 $\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor$个正数。

再看$\frac{h}{p}-\frac{k}{q}<0$，也就是$k$确定后，共有$\left\lfloor\frac{kp}{q}\right\rfloor$个 h 使$\frac{h}{p}-\frac{k}{q}$ 成负数，所以共有$\sum_{k=1}^{q'}\left\lfloor\frac{kp}{q}\right\rfloor$个负数，于是

$$\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor+\sum_{k=1}^{q'}\left\lfloor\frac{kp}{q}\right\rfloor=\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$$

所以

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\sum_{h=1}^{p'}\left\lfloor\frac{hq}{p}\right\rfloor+\sum_{k=1}^{q'}\left\lfloor\frac{kp}{q}\right\rfloor}=(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$$

例 1-32　若奇素数 p 和 q 均满足 $p\equiv 3\pmod 4$，$q\equiv 3\pmod 4$，则$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$。

例 1-33　p、q 中只要有一个满足比如 $p\equiv1(\bmod 4)$，则 $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$。

证　令 $p=4k+3, q=4l+3$，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{2}(4k+3-1)\cdot\frac{1}{2}(4l+3-1)}=-1$$

乘 $\left(\frac{p}{q}\right)$ 得

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$$

若 $p=4k+1$，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{4k+1-1}{2}\cdot\frac{q-1}{2}}=(-1)^{2k\cdot\frac{q-1}{2}}=1$$

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

例 1-34　判断同余式 $x^2\equiv438(\bmod 593)$ 是否有解。

解：593 是素数，$438=2\times3\times73$，所以

$$\left(\frac{438}{593}\right)=\left(\frac{2}{593}\right)\left(\frac{3}{593}\right)\left(\frac{73}{593}\right),$$

$$\left(\frac{2}{593}\right)=(-1)^{\frac{1}{8}(593^2-1)}=(-1)^{\frac{1}{8}(592\times594)}=(-1)^{74\times594}=1,$$

$$\left(\frac{3}{593}\right)=(-1)^{\frac{1}{2}(593-1)\cdot\frac{1}{2}(3-1)}\left(\frac{593}{3}\right)=\left(\frac{2}{3}\right)=(-1)^{\frac{1}{8}(3^2-1)}=-1,\quad(593=197\times3+2)$$

$$\left(\frac{73}{593}\right)=(-1)^{\frac{1}{2}(593-1)\cdot\frac{1}{3}(73-1)}\left(\frac{593}{73}\right)=\left(\frac{9}{73}\right)=\left(\frac{3^2}{73}\right)=-1,\quad(593=73\times8+9)$$

所以 $\left(\frac{438}{593}\right)=-1$，同余式 $x^2\equiv438(\bmod 593)$ 无解。

例 1-35　试求什么样的素数以 3 为平方剩余？

解：$p>3$ 素数，使 $\left(\frac{3}{p}\right)=1$，$\left(\frac{3}{p}\right)=(-1)^{\frac{1}{2}(3-1)\cdot\frac{1}{2}(p-1)}\left(\frac{p}{3}\right)=(-1)^{\frac{1}{2}(p-1)}\left(\frac{p}{3}\right)$。

这就要求 $(-1)^{\frac{1}{2}(p-1)}$ 和 $\left(\frac{p}{3}\right)$ 应同为 $+1$ 或同时为 -1，由 $(-1)^{\frac{1}{2}(p-1)}=1$，得 $p\equiv1(\bmod 4)$，而 $\left(\frac{p}{3}\right)=1$，得 $p\equiv1(\bmod 3)$，于是 $p\equiv1(\bmod 12)$。

由 $(-1)^{\frac{1}{2}(p-1)}=-1$，得 $p\equiv-1(\bmod 4)$，而 $\left(\frac{p}{3}\right)=-1$，得 $p\equiv-1(\bmod 3)$，于是 $p\equiv-1(\bmod 12)$。

所以 3 是 p 的平方剩余必须是 $p\equiv\pm1(\bmod 12)$。

1.23　Jacobi 符号

Jacobi 符号是勒让德符号的推广。

定义 1-10：设 n 是一奇正整数，其素数展开式为

$$n = p_1^{l_1} p_2^{l_2} \cdots p_m^{l_m}$$

令 a 和 n 互素，Jacobi 符号 $\left(\frac{a}{n}\right)$ 定义如下：

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{l_1} p_2^{l_2} \cdots p_m^{l_m}}\right) = \left(\frac{a}{p_1}\right)^{l_1} \left(\frac{a}{p_2}\right)^{l_2} \cdots \left(\frac{a}{p_m}\right)^{l_m}$$

等式左端是 Legender 符号

例 1-36　$\left(\frac{2}{45}\right) = \left(\frac{2}{3^2 \times 5}\right) = \left(\frac{2}{3}\right)^2 \times \left(\frac{2}{5}\right) = (-1)^2 \times (-1) = -1$，当 n 是素数时 Jacobi 符号和 Lenender 符号一样，但 n 是合数时，$\left(\frac{a}{n}\right)$ 不告诉我们 $x^2 \equiv a \pmod n$ 有解。

无论如何 n 是合数 $\left(\frac{a}{n}\right)$ 不告诉 $x^2 \equiv a \pmod n$ 是否有解。

假如 p 是 n 的因子，$x^2 \equiv a \pmod n$ 有解，$x^2 \equiv a \pmod p$ 也有解。$\left(\frac{a}{p}\right) = 1$，$\left(\frac{a}{n}\right) = \prod_{j=1}^{m} \left(\frac{a}{p_j}\right) = 1$ 是可能的。

有可能 $\left(\frac{a}{n}\right) = 1$ 但 $x^2 \equiv a \pmod n$ 无解，$a=2$，$n=15$，$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$，但 $x^2 \equiv 2 \pmod{15}$ 无解。

因 $x^2 \equiv 2 \pmod 3$ 和 $x^2 \equiv 2 \pmod 5$ 无解。

定理 1-36：n 是奇正整数，a 、b 与 n 为互素的整数，则

(1) 若 $a \equiv b \pmod n$ 则 $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$。

(2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$。

(3) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$。

(4) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$。

证　令 $n = p_1^{l_1} p_2^{l_2} \cdots p_m^{l_m}$

(1) 若 p 是素数 $p \mid n$，则 $a \equiv b \pmod p$，根据 Legender 符号的定理：若 $a \equiv b \pmod p$，则 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$，因此

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{l_1} \left(\frac{a}{p_2}\right)^{l_2} \cdots \left(\frac{a}{p_m}\right)^{l_m} = \left(\frac{b}{p_1}\right)^{l_1} \left(\frac{b}{p_2}\right)^{l_2} \cdots \left(\frac{b}{p_m}\right)^{l_m} = \left(\frac{b}{n}\right)$$

(2) 根据 Legender 符号的定理 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$，故

$$\left(\frac{ab}{n}\right) = \left(\frac{ab}{p_1}\right)^{l_1} \left(\frac{ab}{p_2}\right)^{l_2} \cdots \left(\frac{ab}{p_m}\right)^{l_m} = \left(\frac{a}{p_1}\right)^{l_1} \left(\frac{b}{p_1}\right)^{l_1} \left(\frac{a}{p_2}\right)^{l_2} \left(\frac{b}{p_2}\right)^{l_2} \cdots \left(\frac{a}{p_m}\right)^{l_m} \left(\frac{b}{p_m}\right)^{l_m}$$

$$= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

(3) 根据 Legender 符号的定理，若 p 是素数，则 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$，故

$$\left(\frac{-1}{n}\right)=\left(\frac{-1}{p_1}\right)^{l_1}\left(\frac{-1}{p_2}\right)^{l_2}\cdots\left(\frac{-1}{p_m}\right)^{l_m}=(-1)^{\frac{l_1(p_1-1)}{2}+\frac{l_2(p_2-1)}{2}+\cdots+\frac{l_m(p_m-1)}{2}}$$

$$n=[1+(p_1-1)]^{l_1}[1+(p_2-1)]^{l_2}\cdots[1+(p_m-1)]^{l_m}$$

因 $p-1$ 是偶数，所以

$$(1+(p_i-1))^{l_i}=(1+l_i(p_i-1))\pmod 4$$

$$[1+(p_i-1)l_i][1+(p_j-1)l_j]\equiv 1+l_i(p_i-1)+l_j(p_j-1)\pmod 4$$

所以

$$n\equiv 1+l_1(p_1-1)+l_2(p_2-1)+\cdots+l_m(p_m-1)\pmod 4$$

$$\frac{n-1}{2}\equiv\frac{l_1(p_1-1)}{2}+\frac{l_2(p_2-1)}{2}+\cdots+\frac{l_m(p_m-1)}{2}\pmod 2$$

故

$$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$$

(4) 若 p 是素数，则 $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$，故

$$\left(\frac{2}{n}\right)=\left(\frac{2}{p_1}\right)^{l_1}\left(\frac{2}{p_2}\right)^{l_2}\cdots\left(\frac{2}{p_m}\right)^{l_m}=(-1)^{\frac{l_1(p_1^2-1)}{8}+\frac{l_2(p_2^2-1)}{8}+\cdots+\frac{l_m(p_m^2-1)}{8}}$$

$$n^2=[1+(p_1^2-1)]^{l_1}[1+(p_2^2-1)]^{l_2}\cdots[1+(p_m^2-1)]^{l_m}$$

但 $p_j^2-1\equiv 0\pmod 8$，故

$$[1+(p_i^2-1)]^{l_i}\equiv 1+l_i(p_i^2-1)\pmod{64}$$

$$[1+l_i(p_i^2-1)][1+l_j(p_j^2-1)]\equiv 1+l_i(p_i^2-1)+l_j(p_j^2-1)\pmod{64}$$

$$n^2\equiv 1+l_1(p_1^2-1)+l_2(p_2^2-1)+\cdots+l_m(p_m^2-1)\pmod{64}$$

$$\frac{n^2-1}{8}\equiv\frac{l_1(p_1^2-1)}{8}+\frac{l_2(p_2^2-1)}{8}+\cdots+\frac{l_m(p_m^2-1)}{8}\pmod 8$$

故

$$\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$$

定理 1-37(互反定理)：n 和 m 是互素的奇正整数，则 $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$。

证　令 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，$n=q_1^{\beta_1}q_2^{\beta_2}\cdots q_r^{\beta_r}$，

$$\left(\frac{m}{n}\right)=\prod_{i=1}^{r}\left(\frac{m}{q_i}\right)^{\beta_i}=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)^{\beta_i\alpha_j}$$

$$\left(\frac{n}{m}\right)=\prod_{j=1}^{s}\left(\frac{n}{p_j}\right)^{\alpha_j}=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)^{\alpha_j\beta_i}$$

所以

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{i=1}^{r}\prod_{j=1}^{s}\left[\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)\right]^{\alpha_j\beta_i}$$

但

$$\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)=(-1)^{\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)}$$

故

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\alpha_j\left(\frac{p_j-1}{2}\right)\beta_i\left(\frac{q_i-1}{2}\right)}=(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\beta_i\left(\frac{q_i-1}{2}\right)}$$

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\beta_i\left(\frac{q_i-1}{2}\right)=\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\sum_{i=1}^{r}\beta_i\left(\frac{q_i-1}{2}\right)$$

因

$$\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\equiv\frac{m-1}{2}\pmod 2$$

$$\sum_{i=1}^{r}\beta_i\left(\frac{q_i-1}{2}\right)\equiv\frac{n-1}{2}\pmod 2$$

故

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\beta_i\left(\frac{q_i-1}{2}\right)\equiv\frac{m-1}{2}\cdot\frac{n-1}{2}\pmod 2$$

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

下面讨论计算 Jacobi 符号有效的算法。

令 a 和 b 是互素正整数，$a<b$，令 $R_0=a$，$R_1=b$。

$R_0=R_1g+2^{S_1}R_2$，S_1 是一非负整数，R_2 是奇正整数且比 R_1 小

$$R_1=R_2q_2+2^{S_2}R_3$$
$$R_2=R_3q_3+2^{S_3}R_4$$
$$\cdots$$
$$R_{n-3}=R_{n-2}q_{n-2}+2^{S_{n-2}}R_{n-1}$$
$$R_{n-2}=R_{n-1}q_{n-1}+2^{S_{n-1}}\times 1$$

其中，S_j 是非负整数，R_j 是奇整数且比 R_{j-1} 小，$j=2,3,\cdots,n-1$。

举例如下：

$$a=401,\quad b=111$$
$$401=111\times 3+2^2\times 17$$
$$111=17\times 6+2^0\times 9$$
$$17=9\times 1+2^3\times 1$$

定理 1-38：令 a 和 b 是正整数，$a>b$，$\left(\frac{a}{b}\right)=(-1)^{S_1\frac{R_1^2-1}{8}+\cdots+S_{n-1}\frac{R_{n-1}^2-1}{8}+\frac{R_1-1}{2}+\frac{R_2-1}{2}+\cdots+\frac{R_n-1}{2}}$。

其中整数 R_j 和 S_j，$j=1,2,\cdots,n-1$ 是以上讨论的互素正整数。

证　由 Jacobi 定理有

$$\left(\frac{a}{b}\right)=\left(\frac{R_0}{R_1}\right)=\left(\frac{2^{S_1}R_2}{R_1}\right)=\left(\frac{2}{R_1}\right)^{S_1}\left(\frac{R_2}{R_1}\right)=(-1)^{S_1\frac{R_1^2-1}{8}}\left(\frac{R_2}{R_1}\right)$$

由互反定理有

$$\left(\frac{R_2}{R_1}\right)=(-1)^{\frac{R_1-1}{2}\cdot\frac{R_2-1}{2}}\left(\frac{R_1}{R_2}\right)$$

所以

$$\left(\frac{a}{b}\right)=(-1)^{\frac{R_1-1}{2}\cdot\frac{R_2-1}{2}+s_1\frac{R_1^2-1}{8}}\left(\frac{R_1}{R_2}\right)$$

同样

$$\left(\frac{R_{j-1}}{R_j}\right)=(-1)^{\frac{R_j-1}{2}\cdot\frac{R_{j+1}-1}{2}+s_j\frac{R_j^2-1}{8}}\left(\frac{R_j}{R_{j+1}}\right)$$

将这些等式连起来，便得$\left(\frac{a}{b}\right)$。

例 1-37　$\left(\frac{401}{111}\right)=(-1)^{2\cdot\frac{111^2-1}{8}+0\cdot\frac{17^2-1}{8}+3\cdot\frac{9^2-1}{8}+\frac{111-1}{2}\cdot\frac{17-1}{2}+\frac{17-1}{2}\cdot\frac{9-1}{2}}=1$。

习　　题

1. 试求下列数偶的 gcd。

(1)(99,100)　(2)(0,11)　(3)(−12,18)　(4)(100,102)

2. a 是正整数，求 $\gcd(a,a+2)$。

3. 若 a 和 b 是正整数，$(a,b)=1$，试证 $(a+b,a-b)=1$ 或 2。

4. 设 a,b,c 是整数，而且 $(a,b)=(a,c)=1$，试证 $(a,bc)=1$。

5. 若 $a_1,a_2,\cdots,a_n$ 是整数，且不全为零，c 是正整数，试证 $(ca_1,ca_2,\cdots,ca_n)=c(a_1,a_2,\cdots,a_n)$。

6. 若 a,b 是正整数，证 $((a^n-b^n)/(a-b),a-b)=(n(a,b)^{n-1},a-b)$。

7. 若 a 和 b 是正整数，$(a,b)=1$，证 $((a^n-b^n)/(a-b),a-b)=(n,a-b)$。

8. 若 a,b,c,d 是整数，b 和 d 是正的，$(a,b)=(c,d)=1$，$\frac{a}{b}+\frac{c}{d}$是一整数，证 $b=d$。

9. 利用欧几里得算法求下列数偶的最大公因数。

(1) (666,1414)　　(2) (20785,44350)

10. 上题中 gcd 表为两个整数的线性结合。

11. 求下列整数集合的 gcd。

(1) 70,98,105　　(2) 280,330,405,490

12. 求第 11 题的 gcd 表为集合中的数的线性结合。

13. 利用 $(a,b)=(a-b,b)$，若 a、b 都是奇数，$a>b$，$(a,b)=(a/2,b/2)$，若 a、b 都是偶数，$(a,b)=(a/2,b)$，若 a 是偶数，利用上面的规则求(2106,8318)。

14. m 和 n 都是正整数，a 是大于 1 的整数，求证 $(a^{m-1}-1,a^n-1)=a^{(m,n)}-1$。

15. m 和 n 都是正整数，$(f_m,f_n)=f_{(m,n)}$，f_m 是第 m 个 Fibonacci 数，$f_n=f_{n-1}+f_{n-2}$，已知 $f_1=f_2=1$。求 f_{10}。

16. 求 4 849 845 的素数分解。

17. 试问什么正整数正好有三个除数？什么正整数正好有 4 个除数？

18. 求 lcm(6,10,15)，lcm(7,11,13)。

19. 若 a,b,c 是正整数，试证

$$\max(a,b,c) = a+b+c-\min(a,b)-\min(a,c)-\min(b,c)+\min(a,b,c)$$

$$\text{lcm}(a,b,c) = \frac{abc(a,b,c)}{(a,b)(a,c)(b,c)}$$

20. 若 a,b,c 是正整数，试证

$$(a,b,c)[ab,ac,bc] = abc$$

$$[a,b,c](ab,ac,bc) = abc$$

$$([a,b],[a,c],[b,c]) = [(a,b),(a,c),(b,c)]$$

21. 试证，若 $a_1,a_2,\cdots,a_n$ 是两两互素的整数，则 $[a_1,a_2,\cdots,a_n]=a_1a_2\cdots a_n$。

22. 若 a,b,c 是整数，$c>0$，$a\equiv b(\text{mod } c)$，则 $(a,b)=(b,c)$。

23. 若 $a_j\equiv b_j(\text{mod } m)$，$j=1,2,\cdots,n$，$m$ 是正整数，a_j,b_j，$j=1,2,\cdots,n$，是整数，则

$$\sum_{j=1}^{n}a_j \equiv \sum_{j=1}^{n}b_j(\text{mod } m),\quad \prod_{j=1}^{n}a_j \equiv \prod_{j=1}^{n}b_j(\text{mod } m)$$

24. p 是素数，a 是正整数，$a^{-1}(\text{mod } p)=a$ 的充要条件是 $a\equiv 1(\text{mod } p)$，$a\equiv -1(\text{mod } p)$。

25. 求下列线性同余方程的解。

(1) $103x\equiv 444(\text{mod } 999)$

(2) $3x\equiv 6(\text{mod } 9)$

(3) $980x\equiv 1500(\text{mod } 1600)$

(4) $15x\equiv 9(\text{mod } 25)$

(5) $128x\equiv 833(\text{mod } 1001)$

(6) $6\,789\,783x\equiv 2\,474\,010(\text{mod } 28\,927\,591)$

26. 求解 $x+y$。

(1) $x\equiv 33(\text{mod } 99)$，$y\equiv 32(\text{mod } 99)$

(2) $x\equiv 8(\text{mod } 98)$，$y\equiv 92(\text{mod } 98)$

(3) $x\equiv 9(\text{mod } 97)$，$y\equiv 42(\text{mod } 97)$

(4) $x\equiv 89(\text{mod } 95)$，$y\equiv 16(\text{mod } 95)$

27. 求下列线性同余方程组的解。

(1) $\begin{cases} x\equiv 1(\text{mod } 2) \\ x\equiv 2(\text{mod } 3) \\ x\equiv 3(\text{mod } 5) \end{cases}$ (2) $\begin{cases} x\equiv 2(\text{mod } 11) \\ x\equiv 3(\text{mod } 12) \\ x\equiv 4(\text{mod } 13) \\ x\equiv 5(\text{mod } 17) \\ x\equiv 6(\text{mod } 19) \end{cases}$

28. 求 $2^{9!}(\text{mod } 5\,157\,437)$。

29. 利用 Fermat 定理求下列线性同余方程的解。

(1) $7x\equiv 12(\text{mod } 17)$ (2) $4x\equiv 11(\text{mod } 19)$

30. 利用 Euler 定理求 $3^{100\,000} \bmod 35$。

31. a 是和 32 760 互素的整数，证 $a^{12}\equiv 1(\text{mod } 32\,760)$。

32. 利用 Euler 定理解下列线性同余方程：

(1) $5x \equiv 3 \pmod{14}$

(2) $3x \equiv 5 \pmod{16}$

(3) $4x \equiv 7 \pmod{15}$

33. 利用 Euler 定理求 7^{1000} 的最后一位数。

34. 利用 Euler 定理求 $5^{1\,000\,000}$ 的十六进制展开的最后一位。

35. 若 a 和 b 是正整数,试证

$$\Phi(ab) = (a,b)\Phi(a)\Phi(b)/\Phi((a,b))$$

36. 若 n 是正整数,证

$$\Phi(2n) = \begin{cases} \Phi(n) & n \text{ 是奇数} \\ 2\Phi(n) & n \text{ 是偶数} \end{cases}$$

37. 若 n 是正合数,$\Phi(n) \mid (n-1)$,则 n 是非平方,至少是三个不同素数的积。

38. $p=101$,key$e=3$,$m=$good morning,$(e,p-1)=1$,$c=m^e \pmod p$,求密文。

39. $p=29$,$e=5$,$c=m^e \pmod p$,求密文:01 0900 12 12 09 24 10 对应的明文。

40. $p=2591$,$e=13$,$c=m^e \pmod p$,求密文为 12 13 0902 0539 1208 1234 1103 1374 对应的明文。

41. 已知 RSA 密码$(e,n)=(3,2669)$,$m=$best wishes,求密文。

42. 已知 RSA 密码$(e,n)=(13,2747)$,密文 c 为:2206 0755 0436 1165 1737,求 m。

43. 证 5 是 6 的原根,2 是 11 的原根。

44. 求模下列整数的原根。

(1) 4　　(2) 5　　(3) 10　　(4) 13　　(5) 18

45. 求下列指数。

(1) 2 模 5 的指数　　(2) 10 模 13 的指数

(3) 10 模 21 的指数　　(4) 9 模 23 的指数

46. 求 $41^2=1681$ 的一个原根。

47. 求 mod 101 的一个原根。

48. 判定 53,59 是否是 mod 179 的原根。

49. 写出 mod 23 关于原根 5 的指标。

50. 求下列同余方程的解。

(1) $3^x \equiv 2 \pmod{23}$　　(2) $13^x \equiv 5 \pmod{23}$

51. 若 p 是一奇素数,a 和 b 是不被 p 除尽的整数,则

(1) 若 $a \equiv b \pmod p$,则 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(3) $\left(\frac{a^2}{p}\right) = 1$

52. 求下列整数的所有平方剩余。

(1) 3　　(2) 8　　(3) 15　　(4) 18　　(5) 13　　(6) 19

53. 计算$\left(\frac{7}{11}\right)$。

(1) 利用 Euler 判定 (2) 利用 Gauss 引理

54. 求$\left(\frac{j}{5}\right)$,$j=1,2,3,4$。

55. 求$\left(\frac{j}{7}\right)$,$j=1,2,3,4,5,6$。

56. 证若 p 是奇素数,则

$$\left(\frac{-3}{p}\right)=\begin{cases}1, & 若\ p\equiv 1\ 或\ 3 \pmod 8\\ -1, & 若\ p\equiv -1\ 或\ -3 \pmod 8\end{cases}$$

57. 若 $n=p_1^{2t_1+1}p_2^{2t_2+1}\cdots p_k^{2t_k+1}p_{k+1}^{2t_{k+1}+1}\cdots p_m^{2t_m+1}$

q 是一素数,$q\nmid n$,则

$$\left(\frac{n}{q}\right)=\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_k}{q}\right)$$

58. 求 $x^2\equiv 1 \pmod{15}$所有的根。

59. 求 $x^2\equiv 207 \pmod{1001}$所有的根。

60. 求下列同余方程不同余的解的数目。

(1) $x^2\equiv 31 \pmod{75}$ (2) $x^2\equiv 16 \pmod{105}$

(3) $x^2\equiv 46 \pmod{231}$ (4) $x^2\equiv 1156 \pmod{3^2 2^3 7^5 11^6}$

61. 计算下面 Legender 符号的值。

(1) $\left(\frac{3}{53}\right)$ (2) $\left(\frac{7}{79}\right)$ (3) $\left(\frac{15}{101}\right)$ (4) $\left(\frac{31}{641}\right)$

(5) $\left(\frac{111}{991}\right)$ (6) $\left(\frac{105}{1009}\right)$

62. $x^2\equiv 1 \pmod{15}$,求所有的解。

63. $x^2\equiv 207 \pmod{1001}$,求所有解。

64. 求 $x^2\equiv 482 \pmod{2773}$ 的解,$2773=47\times 59$。

第 2 章　群论与有限域理论简介

2.1　群　　论

1. 群的定义

设 G 是非空的集合，在 G 上定义一种运算称为乘法用“·”表示它，所定义的运算满足下面 4 个条件。

（1）封闭性。对于属于 G 的任意两个元素 a 和 b，若 $a \cdot b = c$，则 $c \in G$。

（2）结合律成立。若 $a, b, c \in G$，则 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$。

（3）存在单位元 e。即存在单位元 $e \in G$，对 G 中任意元素 a，恒有 $a \cdot e = e \cdot a = a$。

（4）存在逆元素。对 G 中的任一元素 a，必存在 a^{-1}，使 $a \cdot a^{-1} = a^{-1} \cdot a = e$。

例 2-1　$G = \{0, 1, 2, \cdots, n-1\}$，mod n 关于加法成群。

（1）封闭性 $a, b \in G, a + b \equiv c \pmod{n}, c \in G$。

（2）结合律显然成立。

（3）单位元 $e = 0 \in G$。

（4）存在逆元素 $\forall a \in G, n - a \in G, a^{-1} \pmod{n} = n - a \in G$。

例 2-2　$G = \{1, 2, \cdots, p-1\}$，$p$ 是素数，关于 mod p 的乘法，G 成群。

（1）封闭性 $a, b \in G, a \cdot b \pmod{p} \equiv c$，则 $c \in G$。

（2）结合律显然成立。

（3）单位元 $e = 1, \forall a \in G, a \cdot e = e \cdot a = a$。

（4）逆元素，根据 Fermat 定理：$a^{p-1} \equiv 1 \pmod{p}$，故 $a^{-1} = a^{p-2} \pmod{p} \in G$。

例 2-3　矩阵 $T_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$，$\alpha$ 为任意实数，$G = \{T_\alpha\}$ 成群。

（1）封闭性成立：

$$\begin{aligned} T_\alpha \cdot T_\beta &= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} \\ &= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & \cos\alpha\sin\beta + \sin\alpha\cos\beta \\ -\cos\alpha\cos\beta - \sin\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha+\beta) & \sin(\alpha+\beta) \\ -\sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} = T_{(\alpha+\beta)} \end{aligned}$$

（2）结合律成立：

$$T_\alpha \cdot (T_\beta \cdot T_\gamma) = (T_\alpha \cdot T_\beta) \cdot T_\gamma = T_{\alpha+\beta+\gamma}$$

（3）单位元：

$$e=\begin{pmatrix}\cos 0 & \sin 0\\ -\sin 0 & \cos 0\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=T_0\in G, T_\alpha\cdot T_0=T_0\cdot T_\alpha=T_\alpha$$

（4）逆元素：

$$\forall\, T_\alpha\in G,\quad T_{-\alpha}\in G,\quad T_\alpha\cdot T_{-\alpha}=T_0$$

2. 置换群

设 $A=\{a_1,a_2,\cdots,a_n\}$，$\sigma=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n)\end{pmatrix}$表示 a_i 被 $\sigma(ai_1)$ 所取代，$i=1,2,\cdots,n$。n 个元素的全排列共 $n!$ 个，对应于 $n!$ 个排列的置换成群，称为 n 阶的对称群。

$n=3$ 时，1,2,3 的全排列有 123,132,213,231,312,321。

对应的置换有

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

下面以$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$和$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$的乘法为例，介绍置换的乘法。

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\cdot\begin{pmatrix}3&2&1\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

置换群 6 个置换作乘法详细如表 2-1 所示。

表 2-1　置换群 6 个置换群乘法列表

→	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

从表 2-1 可见：

（1）封闭性成立。

（2）可结合性可验证其成立，留作练习。

（3）单位元$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$。

（4）逆元素：

$$\begin{pmatrix}1 & 2 & 3\\ \sigma(1) & \sigma(2) & \sigma(3)\end{pmatrix}^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \sigma(3)\\ 1 & 2 & 3\end{pmatrix}$$

$$\begin{pmatrix}1 & 2 & 3\\ \sigma(1) & \sigma(2) & \sigma(3)\end{pmatrix}\begin{pmatrix}\sigma(1) & \sigma(2) & \sigma(3)\\ 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$$

比如$\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$的逆$\begin{pmatrix}3 & 1 & 2\\ 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$。

必须指出置换群的乘法，不可交换，比如

$$\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}3 & 1 & 2\\ 3 & 2 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}2 & 1 & 3\\ 1 & 3 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

$$\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\neq\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

交换律成立的群称为 Abel 群或交换群。

上面以 $n=3$ 证明了 S_3 成群，实际上可类似证 S_n成群，置换可用简单的轮换来表示，比如$\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$可用(13)(2)或(13)，即 1 被 3 取代，3 被 1 取代，2 不动，即

$$\begin{pmatrix}a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n\\ a_2 & a_3 & a_4 & \cdots & a_n & a_1\end{pmatrix}=(a_1a_2\cdots a_n)$$

可证

$$(1\quad 2\quad 3\quad 4)=(1\quad 2)(1\quad 3)(1\quad 4)$$

$$\begin{aligned}(1\quad 2)(1\quad 3)(1\quad 4)&=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 3 & 4\end{pmatrix}\begin{pmatrix}1 & 3 & 2 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}\begin{pmatrix}1 & 4 & 2 & 3\\ 4 & 1 & 2 & 3\end{pmatrix}\\ &=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 3 & 4\end{pmatrix}\begin{pmatrix}2 & 1 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}\begin{pmatrix}2 & 3 & 1 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}\\ &=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}\begin{pmatrix}2 & 3 & 1 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}\\ &=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}=(1\quad 2\quad 3\quad 4)\end{aligned}$$

即一个置换可用对称的乘积来表示，对换的奇偶数由置换 p 唯一来确定，比如 $(1\quad 2\quad 3\quad 4)$ 由三个对换的乘积是奇置换。

定理 2-1：S_n 的偶置换全体构成阶为$\frac{1}{2}n!$的子群 A_n。

证　偶置换与奇置换的乘积是奇置换，偶置换与偶置换的乘积是偶置换，所以封闭性成立；可结合律对偶置换成立；单位元$(1)(2)\cdots(n)$ 是偶置换，偶置换的逆还是偶置换，所以 A_n 成群，阶为$\frac{1}{2}n!$。

现将 S_3，A_3，S_4，A_4 罗列于下。

S_3：(1)(2)(3)，(23)，(12)，(13)，(123)，(132)。

A_3：(1)(2)(3)，(123)，(132)。

S_4：(1)(2)(3)(4)，(12)，(13)，(14)，(23)，(24)，(34)，(123)，(124)，(132)，(134)，(142)，(143)，(234)，(243)，(1234)，(1243)，(1324)，(1342)，(1423)，(1432)，(12)(34)，(13)(24)，(41)(23)。

A_4：(1)(2)(3)(4)，(123)，(124)，(132)，(134)，(142)，(143)，(234)，(243)，(12)(34)，(14)(23)，(13)(24)。

3. 群的基本性质

定理 2-2：群的单位元是唯一的。

证 如若不然，设 e_1 和 e_2 都是群 G 的单位元，$e_1e_2=e_1$，$e_1e_2=e_2$，所以 $e_1=e_2$。

定理 2-3：若 $ab=ac$，则 $b=c$；若 $ba=ca$，则 $b=c$。

证 若 $ab=ac$，$\forall a\in G$，存在 a^{-1}，使 $a^{-1}a=e$，用 a^{-1} 作用于 $ab=ac$ 的等号两端，根据结合律成立，所以$(a^{-1}a)b=(a^{-1}a)c$，所以 $b=c$。

类似的方法证 $ba=ca$，则 $b=c$，即用 a^{-1} 右乘于 $ba=ca$ 等号两端，即得 $b=c$。

定理 2-4：群的每个元素的逆元素是唯一的。

证 如若不然，a 的逆元素有 a_1^{-1} 和 a_2^{-1}，$aa_1^{-1}=e$，$aa_2^{-1}=e$，$aa_1^{-1}=aa_2^{-1}$，故 $a_1^{-1}=a_2^{-1}$。

定理 2-5：$(ab\cdots lmn)^{-1}=n^{-1}m^{-1}l^{-1}\cdots b^{-1}a^{-1}$。

证 $(ab\cdots lmn)(n^{-1}m^{-1}l^{-1}\cdots b^{-1}a^{-1})=(ab\cdots lm)(nn^{-1})(m^{-1}l^{-1}\cdots b^{-1}a^{-1})=(ab\cdots lm)(m^{-1}l^{-1}\cdots b^{-1}a^{-1})=\cdots=(aa^{-1})=e$

根据定理，群的元素的逆元素是唯一的，定理证毕。

定义 2-1：群 G 是一个群，H 是 G 的子集，而且 H 关于 G 的乘法也构成群，则称 H 是 G 的子群。

定义 2-2：群 G 的元素的指数，对群 G 的每一个元素 a，存在最小的正整数 k，使 $\underbrace{aa\cdots a}_{k个}=a^k=e$，则称 k 为元素 a 的指数。

例 2-4 S_4 中的元素(1234)，(1234)(1234)=(13)(24)，(13)(24)(1234)=(1432)，(1432)(1234)=(1)(2)(3)(4)，故(1234)的指数是 3。

4. 循环群

若 g 是 G 群的元素，g 的指数是 k，即 $g^k=e$，则 $S=\{g,g^2,\cdots,g^{k-1},g^k=e\}$。则 S 是 G 的子群，或 S 是由 g 为生成元素的循环子群，若 G 群的所有元素都可表示某一元素的幂，则 G 群本身就是循环子群。

$x^{12}=1$ 有 12 个根：

$$\xi_k=e^{\frac{2k\pi i}{12}}\quad(k=1,2,\cdots,12)$$

$$I_{12}=\{e^{\frac{1}{6}\pi i},e^{\frac{1}{3}\pi i},e^{\frac{1}{2}\pi i},e^{\frac{2}{3}\pi i},e^{\frac{5}{6}\pi i},e^{\pi i},e^{\frac{7}{6}\pi i},e^{\frac{4}{3}\pi i},e^{\frac{3}{2}\pi i},e^{\frac{5}{3}\pi i},e^{\frac{11}{6}\pi i},e^{2\pi i}\}$$

是关于复数的乘法构成群，有一阶子群 $\{e^{2\pi i}\}$；二阶子群 $\{e^{2\pi i},e^{\pi i}\}$；三阶子群

$\{e^{2\pi i}, e^{\frac{2}{3}\pi i}, e^{\frac{4}{3}\pi i}\}$，四阶子群$\{e^{2\pi i}, e^{\frac{2}{4}\pi i}, e^{\pi i}, e^{\frac{3}{2}\pi i}\}$；六阶子群$\{e^{2\pi i}, e^{\frac{1}{6}\pi i}, e^{\frac{2}{3}\pi i}, e^{\pi i}, e^{\frac{4}{3}\pi i}, e^{\frac{5}{3}\pi i}\}$。

关于循环群的构造：

(1) $a \in G$，a 的指数为 n，$a^m = e$ 的充要条件 $n | m$。

证　用反证法，假定 m 不是 n 的倍数，设 $m = qn + r$，$0 \leqslant r < n$。

$a^m = a^{qn+r} = a^{qn} \cdot a^r = e \cdot a^r = a^r$，$a^r = a^m = e$，这与 a 的指数为 n 的假定相矛盾。

反之，若 $m = qn$，则 $a^m = (a^n)^q = e^q = e$。

(2) $a, b \in G$，设 a 的指数为 n_1，b 的指数为 n_2，且 $(n_1, n_2) = 1$，则 ab 的指数为 $n_1 n_2$。

证　ab 的指数为 $n_1 n_2$。

$$(ab)^{n_1 n_2} = (a^{n_1})^{n_2} (b^{n_2})^{n_1} = e$$

设 ab 的指数为 n，则 $n | n_1 n_2$，$(ab)^n \cdot b^{-n} = b^{-n}$，而且 $a^n = b^{-n}$，同理可得 $a^{-n} = b^n$，$b^{nn_1} = a^{-nn_1} = e$。

同理 $a^{nn_2} = b^{-nn_2} = e$。

故 $n_1 | nn_2$，$(n_1, n_2) = 1$，故 $n_1 | n$，同理 $n_2 | n$，则 $n = \mathrm{lcm}(n_1, n_2) = \ln n_1 n_2$，又 $n_1 n_2 | n$，$n | n_1 n_2$，所以 $n = n_1 n_2$。

(3) 若 a 的指数为 n，则 a^k 的指数为 $\frac{n}{(n,k)}$。

证　由 $a^{kn} = (a^n)^k = (e)^k = e$，可见 a^k 的指数不超过 n，设 a^k 的指数为 m，m 是使 $(a^k)^m = e$ 的最小正整数。

$(a^k)^{\frac{n}{(n,k)}} = (a^n)^{\frac{k}{(n,k)}} = e$，所以 $m \left| \frac{n}{(n,k)} \right.$。

又 $(a^k)^m = e$，a 的指数为 n，所以 $n | km$。

所以 km 是 k 和 n 的公倍数，故存在一正整数 l 使 $km = l\frac{kn}{(k,n)}$，$m = l\frac{n}{(k,n)}$，$(a^k)^{\frac{n}{(n,k)}} = e$，所以 $l = 1$，$m = \frac{n}{(n,k)}$。

推论　n 阶循环群的每一个元素的指数是 n 的因数。

定义 2-3：n 阶循环群中指数为 n 的元素，称为 n 次原根，$n = p$ 时，p 是一素数，有 $p - 1$ 个原根，一般有 $\Phi(n)$ 个原根。

5. 陪集与商群

定义 2-4：设 H 是 G 的子群，a_1 为在 G 中但不在 H 中的一元素，用 a_1 右乘 H 中的一切元素，$Ha_1 = \{ha_1 | h \in H\}$，则称 Ha_1 为 H 在 G 的一个右陪集。同样可定义 $a_1 H$ 为 H 在 G 的一个左陪集。

若存在 $a_2 \in G$，$a_2 \notin Ha_1$ 同样产生 Ha_2 为 H 在 G 的又一个右陪集，可以证明 $Ha_1 \cap Ha_2 = \varnothing$，即 Ha_1 和 Ha_2 的交集是空集。

若 G 是有限群，可通过有限的以上步骤得

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_r,\quad Ha_i \cap Ha_j = \varnothing,\quad i,j = 1,2,\cdots,r,\quad i \neq j。$$

同样可作左陪集的分解：

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

子群和陪集有如下性质。

(1) Ha 的元素个数和 H 一样多，$|G| = r|H|$。

(2) $a \in G$，而 $a \in Ha$，则称 a 为陪集 Ha 的代表。

(3) 对于 Ha 中任一元素 b，恒有 $Ha = Hb$。

(4) $Ha = Hb$ 的充要条件：$ab^{-1} \in H$。

(5) 类似的讨论适用于左陪集。

6. 群的同构和同态

1) 同构

G_1 和 G_2 是两个群，若 G_1 和 G_2 间存在一个一一对应的满映射 f，而且保持群的运算不变，即 G 群有两个元素 a 和 b，其乘积的映射等于两个元素映射的乘积，即 $f(ab) = f(a)f(b)$，则称两个群 G_1 和 G_2 同构，用 $G_1 \cong G_2$ 表示，如图 2-1 所示。

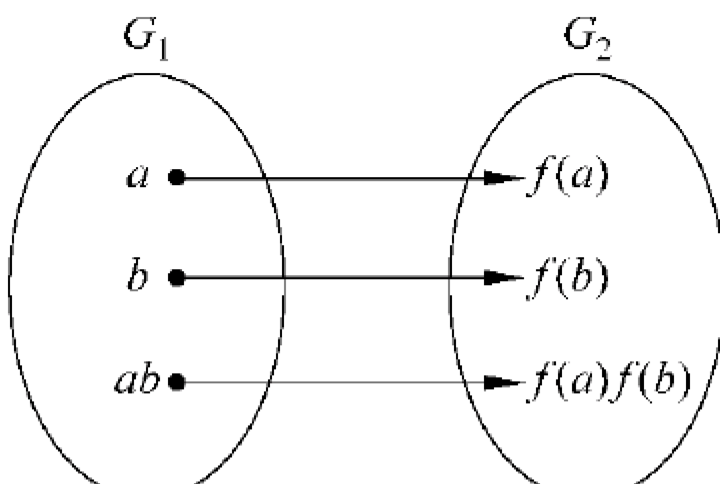


图 2-1 群的同构

同构具有以下性质。

(1) $G \cong G$。

(2) 若 $G_1 \cong G_2$，$G_2 \cong G_3$，则 $G_1 \cong G_3$。

(3) 若 $G_1 \cong G_2$，则映射 f 将 G_1 的单位元映射为 G_2 的单位元。

(4) 若 $G_1 \cong G_2$，则 $G_2 \cong G_1$。

(5) f 将 G_1 的群元素 a 的逆元素映射为 G_2 群 $f(a)^{-1}$。

(6) G_1 群的元素 a 的指数也是 $f(a)$的指数。

(7) 若群 G 是可交换的，则 $f(a)f(b) = f(b)f(a)$。

(8) 设 $G \cong G_1$，H 是 G 的子群的充要条件 $f(H)$是 $f(G)$的子群。

例 2-5 $G = (a_1, a_2\ a_3, a_4)$，$G_1 = \{e, (12)(34), (13)(24), (14)(23)\}$，$G \cong G_1$，可见存在 f：使 $f(a_1) = e$，$f(a_2) = (12)(34)$，$f(a_3) = (13)(24)$，$f(a_4) = (14)(23)$。

可以验证下面右边的 G_1 群的运算成立。

•	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_1	a_4	a_3
a_3	a_3	a_4	a_1	a_2
(a_4)	a_4	a_3	a_2	a_1

G_1

$\overset{f}{\Leftrightarrow}$

•	e	(12)(34)	(13)(24)	(14)(23)
(12)(34)	e	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	e	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	e	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	e

G_1

2) 同态

若存在从群 G 到 G_1 的满映射 F，F 保持群的乘法规则不变，则称 G 和 G 为同态，用

$G \backsim G$ 表示，如图 2-2 所示。

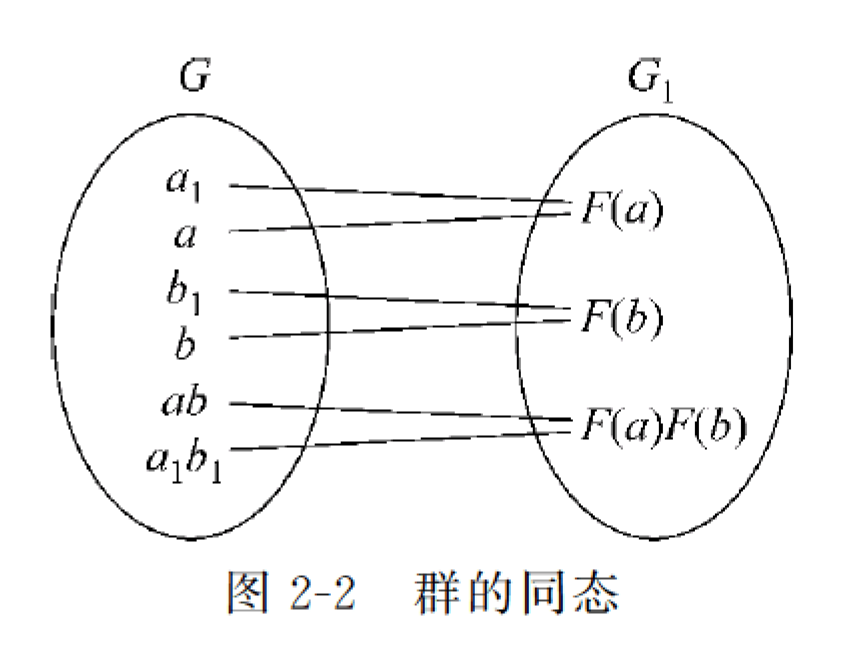


图 2-2　群的同态

同构是特殊的同态，但同态不一定是同构。

若 $G \backsim G_1$，G 中与 G_1 群的单位元素对应的元素集合 K，称为同态核，$K=\{a \in G \mid F(a)=e\}$。

定理 2-6：f：$G \backsim G_1$，f 是同构的充要条件是 $K=\{e\}$。

证　必要条件显然成立，只要证充分条件。假定 $K=\{e\}$，证 f 是一对一的映射，如若不然，$f(a)=f(b)$，$a,b \in G$，即 a,b 在 f 的映射下的像是同一个，根据群的同构的性质，a 的逆元素映射到 G_1 是 $f(a)$ 的逆元素，$f(ab^{-1})=f(a)f(b)^{-1}=e$，$ab^{-1} \in K$，$K=\{e\}$，故 $ab^{-1}=e$，$a=b$，所以 f 是一一对应。

3）正规子群与商群

设 f 是由群 G 到群 G_1 的同态映射，$K=\{a \in G \mid F(a)=e_1\}$，$e_1$ 是 G_1 的单位元，K 是 G 的一个子群，K 是同态核的特点是 aK 和 Ka 在 f 作用下的像都是 $f(a)$，设 H 是 G 的子群，G 对 H 的左陪集分解和 G 对 H 的右陪集分解是一致的，则称 H 为 G 的正规子群。

交换群的子群就是正规子群。

H 对 G 的陪集分解：

$$G = H \cup Ha_1 \cup \cdots \cup Ha_r$$

则 H 是 G 到 G_1 同态映射的核，G_1 的元素：$f(e),f(a_1),\cdots,f(a_r)$，由于 f 是同态映射，$f(a_1a_2)=f(a_1)f(a_2)$。

为了证明 H 是同态映射的核，作陪集元素的集合 $F=\{H,Ha_1,\cdots,Ha_r\}$，定义 F 中的运算：$Ha_iHa_j=Ha_ia_j$，Ha_ia_j 是 H 的一个陪集，证 F 在定义的运算下成群。

（1）封闭性成立。

（2）$(Ha_i \cdot Ha_j)Ha_k=(Ha_ia_j)Ha_k=H(a_ia_j)a_k=Ha_i(a_ja_k)=Ha_iHa_ja_k$
$=Ha_i(Ha_ja_k)=Ha_i(Ha_jHa_k)$。

（3）He 就是 F 的单位元。

（4）若 $a_i^{-1} \in Ha_j$，则 $Ha_iHa_i^{-1}=H=He$，$(Ha_i)^{-1}=Ha_j^{-1}$。

因 F 作为陪集的集合成群，称为 G 对 H 的商群，表示为$\dfrac{G}{F}$。

2.2　有　限　域

1. 有限域的定义

定义 2-5：集合 $F=\{a,b,\cdots\}$，对 F 的元素定义"＋"、"*"，并满足以下三个条件：

（1）F_1：F 的元素关于"＋"运算构成交换群，令其单位元为 O。

（2）F_2：$F\backslash\{0\}$的元素，关于运算"*"构成交换群。

（3）F_3：分配律成立，即 $a,b,c \in F$，$a*(b+c)=a*b+a*c$。

例如，p 是素数时 $F=\{0,1,2,\cdots,p-1\}$关于 mod p 的加法（＋）及乘法（*）构成域，元素数目有限，故为有限域。

例 2-6　$p=5, F=\{0,1,2,3,4\}$，在 mod 5 的意义下关于“+”及“*”构成域

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

例 2-7　$F=\{0,1,2,\cdots,p-1\}$，p 是素数，在 mod p 的意义下关于“+”和“*”构成域，称为 Galois 域，记以 $GF(p)$。

最简单的 $GF(2)$，即 $GF(2)=\{0,1\}$。

例 2-8　$F=\{0,1,x,1+x,x^2,1+x^2,x+x^2,1+x+x^2\}$，在 $GF(2)$ 上关于“+”构成交换群。在 $\bmod(1+x+x^2)$ 意义下，$F\backslash\{0\}$ 关于“*”法构成交换群

*	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
1	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
x	x	x^2	$x+x^2$	$1+x$	1	$1+x+x^2$	$1+x^2$
$1+x$	$1+x$	$x+x^2$	$1+x^2$	$1+x+x^2$	x^2	1	x
x^2	x^2	$1+x$	$1+x+x^2$	$x+x^2$	x	$1+x^2$	1
$1+x^2$	$1+x^2$	1	x^2	x	$1+x+x^2$	$1+x$	$x+x^2$
$x+x^2$	$x+x^2$	$1+x+x^2$	1	$1+x^2$	$1+x$	x	x^2
$1+x+x^2$	$1+x+x^2$	$1+x^2$	x	1	$x+x^2$	x^2	$1+x$

以 $(1+x^2)(x+x^2)$ 为例，

$$\begin{aligned}(1+x^2)(x+x^2) &= x+x^2+x^3+x^4 = x(1+x+x^3)+x^3\\ &\equiv x^3(\bmod(1+x+x^3)) \equiv x+1\end{aligned}$$

因

$$\begin{array}{r|l} & \quad x+1 \\ x^3+x+1 & \quad x^4+x^3+x^2+x \\ & -)\quad x^3+x^2+x \\ \hline & \quad x^3 \\ & \quad x^3+x+1 \\ \hline & \quad x+1 \end{array}$$

又如 $(1+x+x^2)(1+x+x^2)=1+x^2+x^4\equiv x+1(\bmod(1+x+x^3))$

因

$$\begin{array}{r|l} & x \\ x^3+x+1 & x^4\quad +x^2\quad +1 \\ & x^4\quad +x^2+x \\ \hline & \quad x+1 \end{array}$$

定义 2-6：在 F 域上一个多项式，不能表示成两个次方低于多项式的多项式的积，则称该多项式为在 F 域是不可化约的。

以 $1+x^2$ 在实数域上是不可化约的，但在 $GF(2)$ 域是可化约的：

$$1+x^2=(1+x)(1+x)$$

x^3+x+1 在 $GF(2)$ 域上是不可化约的，$\bmod(x^3+x+1)$ 构成 $GF(2^3)$ 域：

$$x^0=1,\quad x^1=x,\quad x^2,\quad x^3=x+1,\quad x^4\equiv x^2+x,\quad x^5\equiv x^3+x^2\equiv x^2+x+1,$$
$$x^6=x^3+x^2+x\equiv x^2+1,\quad x^7\equiv x^3+x\equiv 1$$

x^4+x+1 在 $GF(2)$ 域也是不可化约的，$\bmod(x^4+x+1)$ 构成 $GF(2^4)$ 域：

$$x^0=1,\quad x,\quad x^2,\quad x^3,\quad x^4\equiv x+1,\quad x^5=x^2+x,$$
$$x^6=x^3+x^2,\quad x^7\equiv x^4+x^3\equiv x^3+x+1,\quad x^8\equiv x^4+x^2+x\equiv x^2+1,$$
$$x^9\equiv x^3+x,\quad x^{10}\equiv x^4+x^2\equiv x^2+x+1,\quad x^{11}\equiv x^3+x^2+x,$$
$$x^{12}\equiv x^4+x^3+x^2\equiv x^3+x^2+x+1,\quad x^{13}\equiv x^4+x^3+x^2+x\equiv x^3+x^2+1,$$
$$x^{14}\equiv x^4+x^3+x\equiv x^3+1,\quad x^{15}\equiv x^4+x\equiv 1$$

2. 有限域的基本理论

已知 $GF(p^m)$ 是 $GF(2^n)$ 的拓展。

定理 2-7：设 $p^*(x)$ 是系数在 $GF(p)$ 上的 m 次不可化约的多项式，则次方 $\leqslant m-1$，系数在 $GF(p)$ 上的所有多项式，关于 $\bmod\ p^*(x)$ 构成一阶为 p^m 的 $GF(p^m)$ 域。

例 2-9 在 $GF(3)$ 上不可化约多项式 $p^*(x)=x^2+x+2$，$\bmod\ p^*(x)$ 有

$$x^0=1,\quad x,\quad x^2=2x+1,\quad x^3\equiv 2x^2+x\equiv 2(2x+1)+x\equiv 2x+2,$$
$$x^4\equiv 2x^2+2x=2(2x+1)+2x=2,\quad x^5\equiv 2x,\quad x^6\equiv 2x^2\equiv 2(2x+1)=x+2,$$
$$x^7\equiv x^2+2x\equiv(2x+1)+2x=x+1,\quad x^8\equiv x^2+x\equiv(2x+1)+x\equiv 1$$

上述 $GF(3^2)$ 域：$0,1,2,x,x+1,x+2,2x,2x+1,2x+2$ 构成域。

3. 有限域的特征与元素的指数

$GF(p)$ 和 $GF(p^n)$ 都是有限域，$GF(p)$ 是 $GF(p^n)$ 的最小子域，p 作为 $GF(p^n)$ 的特征。

定理 2-8：有限域的元素数目是素数 p 的方幂。

证 1 表示乘法的单位元，$F=\{f_0,f_1,\cdots\}$ 满足 $f_n=f_{n-1}+1$，$f_{mn}=f_m\cdot f_n$，但 F 有限 $f_0,f_1,\cdots$ 第一次出现 $f_k=f_{k+c}$，$f_{k+c}-f_k=f_c$，故 $f_c=0$，$f_0,f_1,\cdots,f_{c-1}$ 全部不相同，c 就是 F 的特征，c 必然是素数，如若不然，$c=ab$，$1\leqslant a\leqslant c$，$f_c=f_af_b$，$f_c=0$，$f_a\neq 0$，$f_b\neq 0$，这是不可能。

元素的指数定义：$a\in F$，存在使 $a^t\equiv 1$ 的最小正整数 t，t 便称为 a 的指数。

例 2-10 $GF(11)=\{0,1,2,\cdots,10\}$，$3\in GF(11)$，$3^1\equiv 3$，$3^2\equiv 4$，$3^3\equiv 27\equiv 5$，$3^4\equiv 81\equiv 4$，$3^5\equiv 243\equiv 1\ (\bmod\ n)$，3 的指数为 5，$5|10$。

例 2-11 $GF(2^3)=\{0,1,x,x+1,x^2,x^2+1,x+x^2,x^2+x+1\}$，

$a=x+1$，$\bmod(x^3+x+1)$，

$(x+1)$，$(x+1)^2=x^2+1$，$(x+1)^3=x^3+x^2+x+1\equiv x^2$，

$(x+1)^4\equiv x^2(x+1)=x^3+x^2=x^2+x+1$，

$(x+1)^5\equiv(x+1)(x^2+x+1)\equiv x^3+1\equiv x$，$(\bmod\ (x^3+x+1))$，

$(x+1)^6\equiv x(x+1)=x^2+x$，$(\bmod\ (x^3+x+1))$，

$$(x+1)^7 \equiv (x^2+x)(x+1) \equiv x^3+x \equiv 1, (\bmod\ (x^3+x+1)),$$

$(x+1)$的指数是 7。

定理 2-9：设 $F(x)$ 是系数在 $GF(p)$ 的 m 次首一多项式，则 $F(x)=0$ 最多有 m 个属于 $GF(p)$ 的不同的根。

证　用数学归纳法，$m=1$，定理是正确的，假定 $F(x)$的次方小于 m 时定理正确，若存在 $d \in GF(p)$ 使 $F(a)=0$，则

$$F(x) = q(x)(x-d)$$

若 $F(x)$有根 $\beta \neq \alpha$，则由 $F(\beta)=0$，因此 $q(\beta)=0$，$q(x)$的次方小于 m，$q(x)=0$ 的根属于 $GF(p)$的不超过 $m-1$ 个，故 $F(x)=0$ 的根属于 $GF(p)$的不超过 m 个。

引一符号 $O(a)$表示 a 的指数。

引理　若 $O(a)=l$，则 $O(a^k)=\dfrac{l}{(k,l)}$。

证　设 $a \neq 0$，$a^s=1$，当而仅当 $O(a) \mid s$。

令 $d=(k,l)$，故 $a^{k\left(\frac{l}{d}\right)}=a^{l\left(\frac{k}{d}\right)}=(a^l)^{\frac{k}{d}}=1$。

故 $O(a^k) \left| \left(\dfrac{l}{d}\right) \right.$，令 $O(a^k)=h$，则 $a^{hk}=1$，$l \mid hk$。又因 $d=(k,l)$，故存在两个整数 α 和 β，使 $d=\alpha k+\beta l$，$dh=\alpha hk+\beta lh$。

因 $l \mid hk$，故 $l \mid dh$，$\left(\dfrac{l}{d}\right) \left| O(a^k) \right.$，所以 $O(a^k)=\dfrac{l}{d}=\dfrac{l}{(k,l)}$。

例 2-12　$F=\{0,1,2,\cdots,10\}$，mod 13 有

$$\beta=2,\quad \beta^2=4,\quad \beta^3 \equiv 8,\quad \beta^4 \equiv 16 \equiv 3,\quad \beta^5 \equiv 6,\quad \beta^6 \equiv 12,$$

$$\beta^7 \equiv 11,\quad \beta^8 \equiv 9,\quad \beta^9 \equiv 5,\quad \beta^{10} \equiv 10,\quad \beta^{11} \equiv 7,\quad \beta^{12} \equiv 1。$$

$$O(2)=12,\quad O(2^2)=\frac{12}{(12,2)}=6,$$

$$O(2^3)=\frac{12}{(12,3)}=4,\quad O(2^4)=\frac{12}{(12,4)}=3,$$

$$O(2^5)=\frac{12}{(12,5)}=12,\quad O(2^6)=\frac{12}{(12,6)}=2,$$

$$O(2^7)=\frac{12}{(12,7)}=12,\quad O(2^8)=\frac{12}{(12,8)}=3,$$

$$O(2^9)=\frac{12}{(12,9)}=4,\quad O(2^{10})=\frac{12}{(12,10)}=6,$$

$$O(2^{11})=12,\quad O(2^{12})=1,$$

$$\beta=2,\quad O(2^h),\quad h=0,1,2,\cdots,12,$$

不存在指数为 5，8，9，10，11 的指数为 12 的有 4 个，即 $O(2)$，$O(2^5)$，$O(2^7)$，$O(2^{11})$。

还是以 $F=\{0,1,2,\cdots,12\}$为例，mod 13 有

$O(1)=1,\quad O(2)=12,\quad O(3)=3:\ 3^2=9,\quad 3^3=27 \equiv 1,$

$O(4)=6:\ 4^2 \equiv 3,\quad 4^3 \equiv 12,\quad 4^4 \equiv 48 \equiv 9,\quad 4^5 \equiv 36 \equiv 10,\quad 4^6 \equiv 40 \equiv 1,$

$O(5)=4:\ 5^2 \equiv 12,\quad 5^3 \equiv 8,\quad 5^4 \equiv 1,$

$O(6)=12,\quad 6^2 \equiv 10,\quad 6^3 \equiv 8,\quad 6^4 \equiv 48 \equiv 9,\quad 6^5 \equiv 54 \equiv 2,\quad 6^6 \equiv 12,$

$6^7 \equiv 72 \equiv 7$，　$6^8 \equiv 42 \equiv 3$，　$6^9 \equiv 18 \equiv 5$，　$6^{10} \equiv 30 \equiv 4$，$6^{11} \equiv 24 \equiv 11$，
$6^{12} \equiv 66 \equiv 1$，
$O(7) = 12$：$7^1 \equiv 7$，　$7^2 \equiv 49 \equiv 10$，　$7^3 \equiv 70 \equiv 5$，　$7^4 \equiv 35 \equiv 9$，
$7^5 \equiv 63 \equiv 11$，　$7^6 \equiv 77 \equiv 12$，　$7^7 \equiv 84 \equiv 6$，　$7^8 \equiv 42 \equiv 3$，
$7^9 \equiv 21 \equiv 8$，　$7^{10} \equiv 56 \equiv 4$，　$7^{11} \equiv 28 \equiv 2$，　$7^{12} \equiv 14 \equiv 1$，
$O(8) = 4$：$8^2 \equiv 64 \equiv 12$，　$8^3 \equiv 96 \equiv 5$，　$8^4 \equiv 40 \equiv 1$，
$O(9) = 3$：$9^2 \equiv 81 \equiv 3$，　$9^3 \equiv 27 \equiv 1$，
$O(10) = 6$：$10^2 \equiv 100 \equiv 9$，　$10^3 \equiv 90 \equiv 12$，　$10^4 \equiv 120 \equiv 3$，
$10^5 \equiv 30 \equiv 4$，　$10^6 \equiv 40 \equiv 1$，
$O(11) = 12$：$11^2 \equiv 121 \equiv 4$，　$11^3 \equiv 44 \equiv 5$，　$11^4 \equiv 55 \equiv 3$，　$11^5 \equiv 33 \equiv 7$，
$11^6 \equiv 77 \equiv 12$，　$11^7 \equiv 132 \equiv 2$，　$11^8 \equiv 22 \equiv 9$，　$11^9 \equiv 99 \equiv 8$，　$11^{10} \equiv 88 \equiv 10$，
$11^{11} \equiv 110 \equiv 6$，　$11^{12} \equiv 66 \equiv 1$，
$O(12) = 2$：$12^2 \equiv 144 \equiv 1$。

例 2-13　$p(x)=x^4+x^3+x^2+x+1$，mod $p(x)$的 $GF(2^4)$ 的 16 个元素：$0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1,x^3,x^3+1,x^3+x,x^3+x+1,x^3+x^2,x^3+x^2+1,x^3+x^2+x,x^3+x^2+x+1$。
其中，$1,x,x+1$ 的指数如下，(mod $(x^4+x^3+x^2+x+1)$)有
$O(1) = 1$，
$O(x) = 5$：x^2，　x^3，　$x^4 \equiv x^3+x^2+x+1$，　$x^5 = x^4+x^3+x^2+x \equiv 1$，
$O(x+1) = 15$：$(x+1)^2 = x^2+1$，　$(x+1)^3 \equiv (x^2+1)(x+1) \equiv x^3+x^2+x+1$，
$(x+1)^4 = (x^2+1)^2 = x^4+1 = x^3+x^2+x$，
$(x+1)^5 \equiv (x+1)(x^3+x^2+x) = x^4+x \equiv x^3+x^2+1$，
$(x+1)^6 \equiv (x+1)(x^3+x^2+1) = x^4+x^2+x+1 \equiv x^3$，
$(x+1)^7 \equiv x^3(x+1) \equiv x^4+x^3 \equiv x^2+x+1$，
$(x+1)^8 \equiv (x+1)(x^2+x+1) = x^3+1$，
$(x+1)^9 \equiv (x+1)(x^3+1) \equiv x^4+x^3+x+1 \equiv x^2$，
$(x+1)^{10} \equiv x^3+x^2$，
$(x+1)^{11} \equiv (x^3+x^2)(x+1) \equiv x^4+x^2 \equiv x^3+x+1$，
$(x+1)^{12} \equiv (x+1)(x^3+x+1) \equiv x^4+x^3+x^2+1 \equiv x$，
$(x+1)^{13} \equiv (x+1)x \equiv x^2+x$，
$(x+1)^{14} \equiv (x+1)(x^2+x) \equiv x^3+x$，
$(x+1)^{15} \equiv (x+1)(x^3+x) \equiv x^4+x^3+x^2+x \equiv 1$。

4. 本原元素和极小多项式，F 是关于 $GF(p)$的 $GF(p^m)$域

$F^* = F \backslash \{0\}$关于乘法构成 Abel 群，也是循环群：$\{1,g,g^2,\cdots,g^r\}$，$r=p^m-1$。这样的元素 g 称为域$GF(p^m)$的本原元素，也就是 F^* 群的生成元素。

上面已证 $GF(p^m)$上元素 α 满足 $x^{p^m}-x\equiv 0$。

若 $M(x)$是系数在 $GF(p)$上首一多项式中次方最低者，使 $M(\alpha)=0$，则称 $M(x)$是 $GF(p^m)$上元素 α 的极小多项式。

例如，$GF(2^4)$，$m(x)=x^4+x+1$，有

(1) 元素 0 的极小多项式为 x。

(2) 元素 1 的极小多项式为 $x+1$。

(3) 本原元素 a 的极小多项式为 x^4+x+1。

(4) 本原元素 a 的逆元素 a^{-1}的极小多项式 x^4+x^3+1。

证 因 $aa^{-1}=1$，所以 $a=(a^{-1})^{-1}$，$[(a^{-1})^{-1}]^4+(a^{-1})^{-1}+1=0$，用$(a^{-1})^4$乘上式得 $(a^{-1})^0+(a^{-1})^3+(a^{-1})^4=0$，故 a^{-1}满足 $x^4+x^3+1=0$。

例 2-14 求 $GF(2^4)$上 a^3 的极小多项式。

设为 $a_1x^4+a_2x^3+a_3x^2+a_4x+a_5=0$，$a_1,a_2,a_3,a_4,a_5$ 是系数，即

$$a_1(a^3)^4+a_2(a^3)^3+a_3(a^3)^2+a_4(a^3)+a_5=0$$

但

$$\begin{aligned}&a^4\equiv a+1,\quad a^5\equiv a^2+a,\quad a^6\equiv a^3+a^2,\quad a^7\equiv a^4+a^3\equiv a^3+a+1,\\&a^8\equiv a^4+a^2+a\equiv a^2+1,\quad a^9\equiv a^3+a,\quad a^{10}\equiv a^4+a^2\equiv a^2+a+1,\\&a^{11}\equiv a^3+a^2+a,\quad a^{12}\equiv a^4+a^3+a^2\equiv a^3+a^2+a+1,\\&a^{13}\equiv a^4+a^3+a^2+a\equiv a^3+a^2+1,\quad a^{14}\equiv a^4+a^3+a\equiv a^3+1,\\&a^{15}\equiv a^4+a\equiv 1。\end{aligned}$$

所以

$$a_1(a^3+a^2+a+1)+a_2(a^3+a)+a_3(a^3+a^2)+a_4(a^3)+a_5=0$$

$$\begin{cases}a_1+a_2+a_3+a_4=0\\a_1+a_3=0\\a_1+a_2=0\\a_1+a_5=0\end{cases}$$

所以

$$a_3+a_4=0,a_1+a_2=0,\quad a_2+a_4=0,\quad a_1+a_3=0$$

若 $a_1=0$，则 $a_2=a_3=a_4=a_5=0$ 不合要求，故 $a_1\neq 0$。

所以 a^3的极小多项式：$x^4+x^3+x^2+x+1=0$，即 $a_2=a_3=a_4=a_1=a_5=1$。

现将 mod (x^4+x+1) 的 $GF(2^4)$ 的 15 个非零元素和它的极小多项式罗列于后：

(1) $\alpha,\alpha^2,\alpha^4,\alpha^8$的极小多项式为 x^4+x+1。

(2) $\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$的极小多项式为 $x^4+x^3+x^2+x+1$。

(3) α^5,α^{10}的极小多项式为 x^2+x+1。

(4) $\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}$的极小多项式为 x^4+x^3+1。

定理 2-10：若 $\beta(x)\in GF(p^m)$，$M(x)$ 是 β 的极小多项式，则 $M(x)$ 是不可化约的。

证 如若不然，$M(x)=M_1(x)M_2(x)$，$M_1(x)$ 和 $M_2(x)$ 的次方都大于 0，$M(\beta)=M_1(\beta)M_2(\beta)=0$，则导致 $M_1(\beta)=0$ 或 $M_2(\beta)=0$，与极小多项式的假定相矛盾。

定理 2-11：若 $\widetilde{M}(x)$ 是系数在 $GF(p)$ 的多项式，$\widetilde{M}(\beta)=0$，则 $M(x)\mid\widetilde{M}(x)$，$M(x)$ 是 β 的极小多项式。

证 如若不然，$\widetilde{M}(x)=q(x)M(x)+r(x)$。

$r(x)$的次方小于 $M(x)$，$\widetilde{M}(\beta)=0$ 导出 $r(\beta)=0$ 导致矛盾，故

$$r(x)=0, \widetilde{M}(x)=q(x)M(x)$$

定理 2-12：$GF(p^m)$ 上某一次方为 d 的首一多项式 $M(x)$，$d|m$，则 $M(x)|x^{p^m}-x$。

证　令 $m=dn$，mod $M(x)$产生一 $GF(p^d)$ 域，并且 $\beta\in GF(p^d)$，使 $M(\beta)=0$，而且 $GF(p^d)$上每一元素也是 $GF(p^m)$的元素，应满足 $x^{p^m}-x=x^{p^d}-x=0$。

这说明 β 既是 $M(x)=0$ 的根，也是 $x^{p^m}-x$ 的根，故 $M(x)|x^{p^m}-x$。

5. 不可化约的多项式

(1) 一次不可化约的多项式，x，$x+1$。

(2) 二次不可化约的多项式，x^2+x+1。

其他二次方多项式，x^2，$x^2+1=(x+1)^2$，$x^2+x=x(x+1)$。

(3) 三次方不可化约多项式：x^3+x^2+1，x^3+x+1。

其他三次方多项式 $x^3+1=(x+1)^3$，$x^3+x=x(x^2+1)=x(x+1)^2$，$x^3+x^2=x^2(x+1)$，$x^3+x^2+x=x(x^2+x+1)$。

(4) 四次方不可化约多项式：x^4+x+1，x^4+x^3+1，$x^4+x^3+x^2+x+1$。

其他四次多项式都可分解。

习　题

1. 请求 S_5 和 A_5。
2. 试证 n 阶循环群的每一个元素，它的指数必是 n 的因数。
3. 试求 p 阶循环群的生成元素，p 是素数。
4. 试对 S_4 群找出子群，并将它分解为左陪集或右陪集。
5. $GF(2^3)$，$m(x)=x^3+x^2+1$，求 $GF(2^3)$ 的各元素，并求其中$(x+1)$ 的指数。
6. $F=\{0,1,2,\cdots,10)$，试求 mod 11 其中各元素的指数。

第 3 章　大 数 分 解

3.1　Pollard $p-1$ 因数分解法

RSA 公钥密码的出现，掀起了人们对大数分解进行研究的热潮，如果 $n=pq$ 被分解成功，则 RSA 系统便被攻破，所以必须选择好 p 和 q，使之分解十分困难或不可能。

近些年来，数学家在大数分解上取得了引人注目的成就。1994 年 4 月，Lenstra 领导的跨国科研群体约 600 人集中了 1600 台计算机在网上联合作战，花费 38 个月的时间，分解成功了被称为 RSA129 的这个长达 129 位的十进制数。

1999 年 8 月，由 6 个国家的科学家组成的团队，将 RSA155 分解成功。

RSA155 = 1 094 173 864 157 052 742 180 970 732 204 035 761 200 373 294 544 920 599 013 842 131 476 349 984 288 934 784 717 997 257 891 267 332 497 625 752 899 781 833 797 076 537 244 027 146 743 531 593 354 333 897

p = 102 639 592 829 741 105 772 054 196 573 991 675 900 716 567 808 038 066 803 341 933 521 790 711 307 779

q = 106 603 488 380 168 454 820 927 220 360 012 878 679 207 958 575 989 291 522 270 608 237 193 062 808 643

对此数学家做了复杂性估计，每增加 10 位十进制数，分解的复杂性将增加 10 倍。按此估计，若 n 取 200 位十进制数将是很安全的。

现在回到 $p-1$ 因数分解法，或 Pollardr $p-1$ 因数分解法。假定要对 n 进行因数分解，p 是 n 的某一个因数，若 $p-1$ 不存在大的素数因子，则下面的方法可供找出因数 p。

S1 选一整数 k，要求 k 为比界 B 小的所有数的倍数，比如 $k=B!$。

S2 在 $2\sim n-2$ 间取一数 a，可以是 2 或 3，也可以是随机的。

S3 计算 a^k，(mod n)。

S4 利用欧几里得算法计算 $d=(a^k,n)$。

S5 若 d 不是 n 的非平凡除数，则重新选择 a 和 k，转 S1 重新开始。

算法的根据是：由于 k 被小于 B 和等于 B 的所有数除尽，p 是 n 的因子，若 $p-1$ 是小于 B 的素数的幂的乘积，则 k 是 $p-1$ 的倍数。根据 Fermat 定理 $a^k\equiv 1 \pmod p$，故

$$p \mid \gcd(a^k-1,n)$$

失败的可能是由于 $a^k\equiv 1$，(mod n)。

例如 $n=540\ 143$，$B=8$，$k=B!=840$，$a=2$，$2^{840} \pmod n \equiv 53\ 047$，

$$540\ 143 = 10 \times 53\ 046 + 9683$$
$$9683 = 540\ 143 - 10 \times 53\ 046$$
$$53\ 046 = 5 \times 9683 + 4631$$
$$4631 = 53\ 046 - 5 \times 9683$$
$$9683 = 2 \times 4631 + 421$$
$$421 = 9683 - 2 \times 4631$$

$4631=11\times421$，所以 $\gcd(53\ 046,540\ 143)=421$，$540\ 143=1283\times421$。

540 143 之所以被因数分解，是由于 $421-1=420=2^2\times3\times7$。

即 540 143 有一因数 421，而 421 的所有因数和幂都是小素数。与 $p-1$ 分解法类似的有 $p+1$ 分解法，即 $p+1$ 可被分解为小素数乘积时，p 是数 n 的因数，n 可被因数分解，即若 $n=r$，$p-1=\prod_{i=1}^{s} p_i^{\alpha_i}$ 或 $p+1=\prod_{j=1}^{s} q_j^{B_j}$。

所有 $p_i\leqslant B$，$q_j\leqslant B$，则 n 可被因子分解。

这里提供一信息，RSA 的 $n=pq$，且要求对 $p-1$ 和 $p+1$ 的所有因数都不是小的数，q 也一样要求 $q-1$，$q+1$ 不存在小的因数。

*3.2　连分数因数分解法

定义 $a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{}{\ddots+\cfrac{1}{a_m}}}}$

用 $[a_0,a_1,a_2,\cdots,a_m]$ 表示，称为连分数，其中 $a_0\in Z$，$a_i\in N$，$1\leqslant i\leqslant m$。若 $m\to\infty$，则表示为 $[a_0,a_1,\cdots]$。

显然，连分数是一有理数。

引理：任一有理数都可以用有限的连分数表示。

证　证明的过程也就是求连分数的步骤，即证明是构造性的。设 $\frac{a}{b}$ 是有理数，令 $s_0=a$，$s_1=b$，$s_i=q_is_{i+1}+s_{i+2}$，$0\leqslant s_{i+2}<s_{i+1}$，$i\geqslant0$，直到 $s_{n+2}=0$ 为止，这时 m 为奇整数，

$$s_m = q_m s_{m+1}$$

所以

$$\frac{a}{b}=\frac{s_0}{s_1}=\frac{q_0s_1+s_2}{s_1}=q_0+\frac{s_2}{s_1}=q_0+\frac{s_2}{q_1s_2+s_3}$$
$$=q_0+\cfrac{1}{q_1+\cfrac{s_3}{s_2}}=q_0+\cfrac{1}{q_1+\cfrac{1}{\cfrac{s_2}{s_3}}}=q_0+\cfrac{1}{q_1+\cfrac{1}{\cfrac{q_2s_3+s_4}{s_3}}}=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{s_4}{s_3}}}=\cdots$$

$$=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{\ddots}{q_{m-1}+\cfrac{s_{m+1}}{s_m}}}}=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{\ddots}{q_{m-1}+\cfrac{1}{q_m}}}}$$

$\frac{a}{b}$ 可以用连分数$[q_0,q_1,\cdots,q_m]$来表示，$q_i>0$，$i>1$。

算法： 已知$\frac{a}{b}$是有理数

S1 $s_0\leftarrow a, s_1\leftarrow b, i\leftarrow 0$。

S2 $s_i=q_i s_{i+1}+s_{i+2}$，$i\leftarrow i+1$。

S3 若 $s_{i+2}=0$，则转 S4，否则转 S2。

S4 输出$[q_0,q_1,\cdots,q_m]$，其中 m 是 $s_{n+2}=0$。

例 3-1 $[1,2,2,2]=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}=1+\cfrac{1}{2+\cfrac{1}{\cfrac{5}{2}}}=1+\cfrac{1}{2+\cfrac{2}{5}}=1+\frac{5}{12}=\frac{17}{12}$

例 3-2 $[-2,2,4,2,4]=-2+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{4}}}}=-2+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{\cfrac{9}{4}}}}$

$$=-2+\cfrac{1}{2+\cfrac{1}{4+\cfrac{4}{9}}}=-2+\cfrac{1}{2+\cfrac{9}{40}}$$

$$=-2+\cfrac{1}{\cfrac{89}{40}}=-2+\frac{40}{89}=-\frac{138}{89}$$

例 3-3 $\frac{17}{12}=1+\frac{5}{12}=1+\cfrac{1}{\cfrac{12}{5}}=1+\cfrac{1}{2+\cfrac{2}{5}}=1+\cfrac{1}{2+\cfrac{1}{\cfrac{5}{2}}}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}=[1,2,2,2]$

例 3-4 $\frac{-138}{89}=-2+\frac{40}{89}=-2+\cfrac{1}{\cfrac{89}{40}}=-2+\cfrac{1}{2+\cfrac{9}{40}}=-2+\cfrac{1}{2+\cfrac{1}{\cfrac{40}{9}}}$

$$=-2+\cfrac{1}{2+\cfrac{1}{4+\cfrac{4}{9}}}=-2+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{\cfrac{9}{4}}}}=-2+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{4}}}}$$

$$=[-2,2,4,2,4]$$

例 3-5

$$\frac{294}{159}=1+\frac{135}{159}=1+\cfrac{1}{\frac{159}{135}}=1+\cfrac{1}{1+\frac{24}{135}}=1+\cfrac{1}{1+\cfrac{1}{\frac{135}{24}}}$$

$$=1+\cfrac{1}{1+\cfrac{1}{5+\frac{15}{24}}}=1+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{\frac{24}{15}}}}=1+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{1+\frac{9}{15}}}}$$

$$=1+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{1+\cfrac{1}{\frac{15}{9}}}}}=1+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{1+\cfrac{1}{1+\frac{6}{9}}}}}$$

$$=1+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{2}}}}}}=[1,1,5,1,1,1,2]$$

假定 n 是待因数分解整数，以下运算都在 mod n 下进行，$b_{-1}\leftarrow 0$，$b_0\leftarrow a_0=\lfloor\sqrt{n}\rfloor$，$x_0\leftarrow\sqrt{n}-a_0$，$b_0^2$，(mod n)。

令 $i=1,2,3,\cdots$，进行以下运算，并观察 b_i^2(mod n)所得各数。

$$a_i\leftarrow\left\lfloor\frac{1}{x_{i-1}}\right\rfloor,\quad x_i\leftarrow\frac{1}{x_{i-1}}-a_i,\quad b_i\leftarrow a_ib_{i-1}+b_{i+1},\quad (\text{mod } n),\quad b_i^2,\quad (\text{mod } n),$$

得一表将它们因数分解成小素数的积，构成因数基 B，对于每个 b_i^2(mod n)，含有属于 B 的因数表以对应向量 β。

例 3-6　求 9073 的因数分解(见表 3-1)。

$i=0$

$$b_{-1}=1,\quad b_0=a_0=\lfloor\sqrt{9073}\rfloor=95,\quad x_0=\sqrt{9073}-95,$$

$$b_0^2\equiv 9025,\quad (\text{mod } n)=-48,\quad (\text{mod } n)$$

$i=1$

$$a_1=\left\lfloor\frac{1}{\sqrt{9073}-95}\right\rfloor=\left\lfloor\frac{\sqrt{9073}+95}{48}\right\rfloor=3,$$

$$x_1=\frac{1}{\sqrt{9073}-95}-3=\frac{\sqrt{9073}+95}{48}-3=\frac{\sqrt{9073}-49}{48},$$

$$b_1=a_1b_0+b_{-1}=3\times 95+1=286$$

$$b_1^2\equiv 81\,796\equiv 139,\quad (\text{mod } n)$$

$i = 2$

$$a_2 = \left\lfloor \frac{48}{\sqrt{9073}-49} \right\rfloor = \left\lfloor \frac{48(\sqrt{9073}+49)}{6672} \right\rfloor = 1,$$

$$x_2 = \frac{48}{\sqrt{9073}-49} - 1 = \frac{97-\sqrt{9073}}{\sqrt{9073}-49},$$

$b_2 = a_2 b_1 + b_0 = 286 + 95 = 381,$

$b_2^2 \equiv 145\,161 \equiv -7, (\bmod n)$

$i = 3$

$$a_3 = \left\lfloor \frac{\sqrt{9073}-49}{97-\sqrt{9073}} \right\rfloor = 26,$$

$$x_3 = \frac{\sqrt{9073}-49}{97-\sqrt{9073}} - 26,$$

$b_3 = a_3 \cdot b_2 + b_1 = 26 \times 381 + 286 = 10\,192 \equiv 1119, (\bmod n),$

$b_3^2 (\bmod n) = 1\,252\,161, (\bmod n) \equiv 87$

$i = 4$

$a_4 = 2,\quad b_4 = 2619, b_4^2, (\bmod n) \equiv -27$

表 3-1　例 3-6 表

p_i \ $b_i^2 (\bmod n)$	-1	2	3	7	87	139
$-48 = -2^4 \times 3$	1	4	1			
139						1
$-7 = -1 \times 7$	1			1		
87					1	
$-27 = -3^3$	1		3			

从表 3-1 可见 $i=0,4$ 时两行分别为(1,4,1,0,0,0)和(1,0,3,0,0,0)。这两行的和均为偶数。

$(b_0^2)(b_4^2) \equiv (-48) \times (-27) = 4^2 \times 9^2, (\bmod 9073),$

$b_0 b_4 = 95 \times 2619 = 248\,805, \quad \equiv 3834, (\bmod 9073),$

$(3834)^2 \equiv (36)^2, (\bmod 9073),$

$\gcd(3834 + 36, 9073) = \gcd(3870, 9073) = 43,$

$9073 = 211 \times 43$

例 3-7　分解 637 753(见表 3-2)。

$i = 0$

$b_{-1} = 1,\quad b_0 = \lfloor \sqrt{637\,753} \rfloor = 798,\quad a_0 = 798,$

$b_0^2 = 636\,804 = 2^2 \times 3^2 \times 1789,$

$x_0 = \sqrt{637\,753} - 798$

$i=1$

$$a_1=\left\lfloor\frac{1}{\sqrt{637\,753}-798}\right\rfloor=1,$$

$$x_1=\frac{1}{\sqrt{637\,753}-798}-1=\frac{799-\sqrt{637\,753}}{\sqrt{637\,753}-798},$$

$$b_1=b_0+b_{-1}=798+1=799,$$

$$b_1^2=638\,401=648,(\mathrm{mod}\ n)$$

$$648=2^3\times 3^4$$

$i=2$

$$a_2=\left\lfloor\frac{\sqrt{637\,753}-798}{799-\sqrt{637\,753}}\right\rfloor=1,$$

$$x_2=\frac{\sqrt{637\,753}-798}{799-\sqrt{637\,753}}-1=\frac{2\sqrt{637\,753}-1597}{799-\sqrt{637\,753}},$$

$$b_2=b_1+b_0=799+798=1597,$$

$$b_2^2=2\,550\,409=-603,(\mathrm{mod}\ n),$$

$$-603=(-1)\times(3)\times(201)=(-1)\times(3)^2\times(67)$$

$i=3$

$$a_3=\left\lfloor\frac{799-\sqrt{637\,753}}{2\sqrt{637\,753}-1597}\right\rfloor=2,$$

$$x_3=\frac{799-\sqrt{637\,753}}{2\sqrt{637\,753}-1597}-2=\frac{3993-3\sqrt{637\,753}}{2\sqrt{637\,753}-1597},$$

$$b_2=2\times 1597+799=3993,$$

$$b_2^2=15\,944\,049\equiv 224,(\mathrm{mod}\ n),\quad 224=2^5\times 7$$

以后的计算不一一给出,只叙述结果。

因数基 $B=\{-1,2,3,7,13,59,67,73\}$

表 3-2　例 3-7 表

$b_i^2(\mathrm{mod}\ n)$ \ p_i	−1	2	3	7	13	59	67	73
-13×73	1				1			1
$2^3 3^4$		1						
$-3^2\times 67$	1						1	
→ $2^5 7$		1		1				
-3×349								
3×149								
-907								
→ $2^3\times 3^2\times 7$		1		1				

表 3-7 中左端→所指的两行对应元素之和构成偶数。

$b_3 \equiv 3993$，$(\bmod\ n)$，$b_7 \equiv 114\ 199$，$(\bmod\ n)$

$3993 \times 114\ 199 \equiv 3212$，$(\bmod\ n)$

$(3212)^2 \equiv 2^8 \times 3^2 \times 7^2 (\bmod\ n)$，即$(3212)^2 \equiv (2^4 \times 3 \times 7)^2$，$(\bmod\ n)$，

$2^4 \times 3 \times 7 = 336$，

$\gcd(3212 + 336, 637\ 753) = \gcd(3548, 637\ 753) = 887$，

$\gcd(3212 - 336, 637\ 753) = \gcd(2876, 637\ 753) = 719$，

$887 \times 719 = 637\ 753$

3.3 Pollard ρ法

Pollardρ 法其基本思想为：选择出数 $f: Z_n \to Z_n$，$x_0 \in Z_n$，$x_i = f(x_{i-1})$，$i>0$，希望序列 $x_0, x_1, x_2, \cdots$ 为 Z_n的独立的随机数序列，如果 p 是 n 的一个素数因子，则 mod p 将会发生碰撞，即有两个整数 t 和 l，$l>0$，使 $x_t \equiv x_{t+l} (\bmod\ p)$。

Pollard ρ 算法：

S1 在$\{0,1,\cdots,n-1\}$中随机取一数 x_0，$y_0 \leftarrow x_0$，$i \leftarrow 0$。

S2 $i \leftarrow i+1$，$x_i \leftarrow x_{i-1}^2 + 1\ (\bmod\ n)$，$y_i \leftarrow (y_{i-1}^2 + 1)^2 + 1\ (\bmod\ n)$。

S3 $g \leftarrow \gcd(x_i - y_i, n)$。

若 $1<g<n$ 则作

始 输出 g，结束**终**，否则作

始 若 $g=n$ 则作

始 输出 $g=n$，结束**终**，否则

转 S2，**终**。

例 3-8 $n=82\ 123$，$x_0 \leftarrow 631$，$y_0 \leftarrow 631$，

$i=1$，$x_1 = 631^2 + 1 = 398\ 162 \equiv 69\ 670$，$(\bmod\ 82\ 123)$，

$y_1 = (69\ 670)^2 + 1 = 4\ 853\ 908\ 901 \equiv 28\ 986$，$(\bmod\ n)$

$x_1 - y_1 = 40\ 684$，

$82\ 123 = 2 \times 40\ 684 + 755$，

$d = (82\ 123, 40\ 684) = (40\ 684, 755)$，

$40\ 684 = 53 \times 755 + 669$，

$d = (40\ 684, 755) = (755, 669)$，

$755 = 669 + 86$，$d = (669, 86)$，

$669 = 7 \times 86 + 67$，$d = (86, 67) = (67, 19) = (19, 10) = (3, 1) = 1$。

$i=2$，$x_2 = 28\ 986$，$y_2 = 13\ 166$，$(28\ 986 - 13\ 166, 82\ 123) = 1$。

$i=3$，$x_3 = 69\ 907$，$y_3 = 40\ 816$，$(x_3 - y_3, n) = 1$。

$i=4$，$x_4 = y_2 = 13\ 166$，$y_4 = 20\ 459$，$(x_4 - y_4, n) = 1$。

$i=5$，$x_5 = 64\ 027$，$y_5 = 6685$，$(x_5 - y_5, n) = 1$。

$i=6$，$x_6 = y_3 = 40\ 816$，$y_6 = 75\ 835$，$(x_6 - y_6, n) = 1$。

$i=7$，$x_7 = 80\ 802$，$y_7 = 17\ 539$，$x_7 - y_7 = 63\ 263$。

$$
\begin{aligned}
d &= (82\,123, 63\,263) = (63\,263, 18\,860) = (18\,860, 6683) = (6683, 5494) \\
&= (5494, 1189) = (1189, 738) = (738, 451) = (451, 287) = (287, 164) \\
&= (164, 123) = (123, 41) = 41, \\
n &= 82\,123 = 41 \times 2003
\end{aligned}
$$

类似地，mod 41 计算如下，$631 \equiv 16$，(mod 41)，

$$
\begin{aligned}
&i = 0, \quad x_0 \leftarrow 16 \\
&i = 1, \quad 16^2 + 1 = 257 \equiv 11, \quad (\text{mod } 41), \quad x_1 \leftarrow 11 \\
&i = 2, \quad 11^2 + 1 = 122 \equiv 40, \quad (\text{mod } 41), \quad x_2 \leftarrow 40 \\
&i = 3, \quad 40^2 + 1 = 1601 \equiv 2, \quad (\text{mod } 41), \quad x_3 \leftarrow 2 \\
&i = 4, \quad x_4 \leftarrow 5 \\
&i = 5, \quad x_5 \leftarrow 26 \\
&i = 6, \quad 26^2 + 1 = 677 \equiv 21, \quad (\text{mod } 41), \quad x_6 \leftarrow 21 \\
&i = 7, \quad 21^2 + 1 = 442 \equiv 32, \quad (\text{mod } 41), \quad x_7 \leftarrow 32 \\
&i = 8, \quad 32^2 + 1 = 1025 \equiv 0, \quad (\text{mod } 41), \quad x_8 \leftarrow 0 \\
&i = 9, \quad x_9 \leftarrow 1 \\
&i = 10, \quad x_{10} = 2
\end{aligned}
$$

具体见图 3-1。

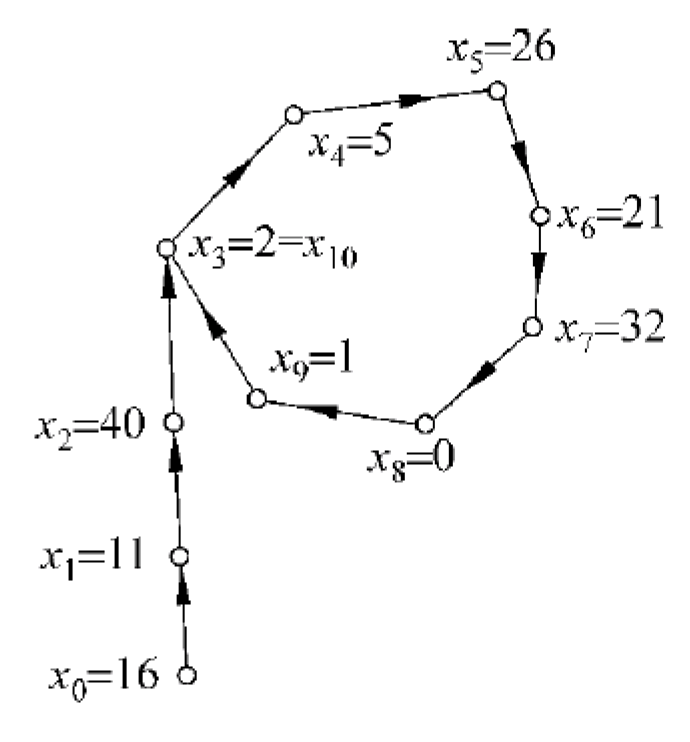


图 3-1　Pollard 迭代举例

3.4　Dixon 随机平方因数分解法

本节将举例说明该算法及其思想。

若

$$
n = s^2 - t^2 = (s-t)(s+t)
$$

$$
n = ab = \left(\frac{a+b}{2}\right)^2 \cdot \left(\frac{a-b}{2}\right)^2
$$

这说明 n 的因数分解和将 n 表示成一对数的平方差相对应。令 $t = \lfloor\sqrt{n}\rfloor, \lfloor\sqrt{n}\rfloor + 1, \cdots$，测试 $t^2 - n$ 是否是一个完全的平方。假如找到 $t^2 - n = s^2$，则 $n = t^2 - s^2$，可利用其来对 n 进行因数分解。若 $n = ab$，而 $a - b$ 的值比较小。

例如，$n=2\,027\,651\,281$，$\sqrt{n}\approx 45\,029$，

$$n=45\,041^2-1020^2=(45\,041+1020)\times(45\,041-1020)=46\,061\times 44\,021。$$

例 3-9　$n=2183$，设能找到以下同余式，

$$453^2\equiv 7,\quad (\mathrm{mod}\ 2183),\quad 1014^2\equiv 3,\quad (\mathrm{mod}\ 2183),\quad 209^2\equiv 21,\quad (\mathrm{mod}\ 2183)$$

则

$$(453\times 1014\times 209)^2\equiv (21)^2,\quad (\mathrm{mod}\ 2183)$$

$$453\times 1014\times 209=96\,002\,478\equiv 687,\quad (\mathrm{mod}\ 2183)$$

所以

$$(687)^2\equiv (21)^2,\quad (\mathrm{mod}\ 2183)$$

$$(687)^2-(21)^2=(687+21)\times(687-21)\equiv 0,\quad (\mathrm{mod}\ 2183)$$

$$687+21=708,\quad 687-21=666$$

令 $d_1=(708,2183)$，$d_2=(666,2183)$，但 $d_1=(708,59)=59$。

$$d_2=(666,185)=(185,111)=(111,74)=(74,37)=37,$$

$$2183=37\times 59$$

关于大数的因数分解更进一步的讨论，还需更上一层楼。

习　　题

试用不同方法分解 200 819。

第 4 章　线性反馈移位寄存器

4.1　流　　码

若能以一种方式产生一随机序列，且由密钥来控制，则可由此序列进行加密，如图 4-1 所示。

密钥k
密钥流产生器
明文m
密码c

图 4-1　流码定义

这样的密码称为序列密码，也叫流码，其中$\oplus$表示 mod 2 的加法。密钥流产生器是给定一种算法产生的密钥流，通常是 0，1 数据流。人们希望它尽可能长，且有随机性，但严格地说它不可能做到完全随机，只能是伪随机。下面给出 Golomb 的随机公设，密钥 0，1 序列，例如 00110111，00 便称为 0 的 2 游程，11 是 1 的 2 游程，接着是 0 的 1 游程，最后是 1 的 3 游程。

假定 0，1 序列$\{s_i\}$，存在r对所有的正整数i都满足$s_i=s_{r+i}$，$i\geqslant 0$，使这等式成立的最小正整数r称为序列$\{s_i\}$的周期。

若有两个子序列$s_1,s_2,\cdots,s_r;s_{1+\tau},s_{2+\tau},\cdots,s_{r+\tau}$。

若s_i和$s_{i+\tau}$相同的数目为n_τ，不相同的数目为$d_\tau=r-n_\tau$，令$R(\tau)=\dfrac{d_\tau-n_\tau}{r}$，$\tau=0$，则$n_\tau=r$，$d_\tau=0$，$R(0)=1$。$\tau\neq 0$，$R(\tau)$为异相自相关函数。

Golomb 提出 0，1 序列的随机性公设：

(1) 若Y是奇数，则 0，1 序列在一个周期内 0 的个数比 1 的个数多一个或少一个。

(2) 在长度为r的周期内，1 的游程的数目为游程总数的$\dfrac{1}{2}$，2 的游程的数目占游程总数的$\dfrac{1}{2^2}$，…，c游程的数目占游程总数的$\dfrac{1}{2^c}$，而且对于任意长度 0 的游程个数和 1 的游程个数相等。

(3) 异相自相关函数是个常数。

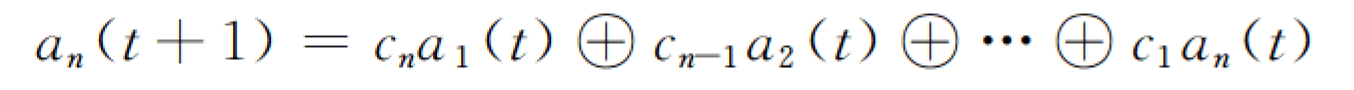
(1)和(2)的意义都较明显，(3)意味着通过对序列与其平移后的序列作比较，不能给出其他任何信息。

4.2　线性反馈移位寄存器

LFSR 是 Linear Feedback Shift Register 的缩写。

如图 4-2 所示标以$a_1,a_2,\cdots,a_n$的小方块是(0，1)二值的寄存器，$a_i(t+1)$表示t时刻a_i寄存器所含的值。

$$a_{i+1}(t)=a_i(t+1)$$



$$a_n(t+1) = c_n a_1(t) \oplus c_{n-1} a_2(t) \oplus \cdots \oplus c_1 a_n(t)$$

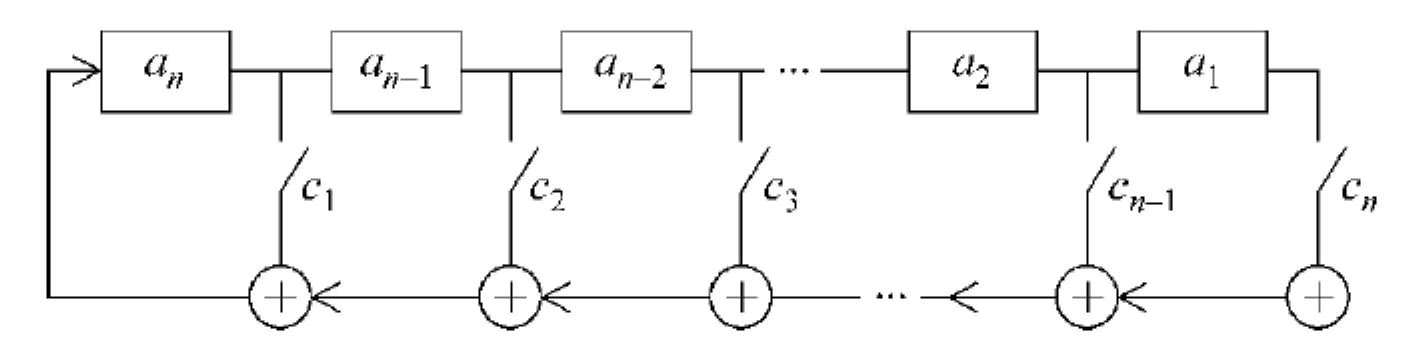


图 4-2　线性反馈移位寄存器(LFSR1)

$c_i=0$ 或 1 表示开关 c_i 分别是打开或闭合。

例如(见图 4-3 与表 4-1)：

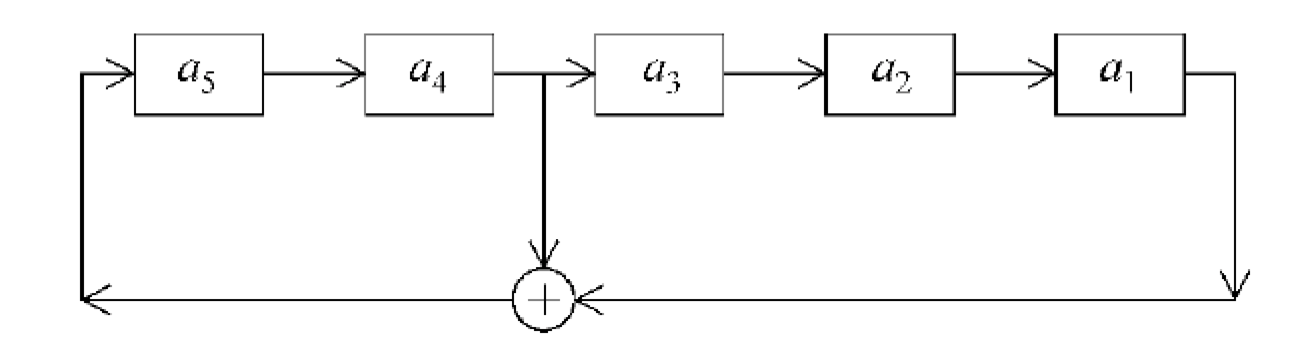


图 4-3　线性反馈移位寄存器(LFSR2)

表 4-1　图 4-3 对应表

i	a_5	a_4	a_3	a_2	a_1	i	a_5	a_4	a_3	a_2	a_1
0	1	0	1	0	1	17	1	1	0	0	1
1	1	1	0	1	0	18	0	1	1	0	0
2	1	1	1	0	1	19	1	0	1	1	0
3	0	1	1	1	0	20	0	1	0	1	1
4	1	0	1	1	1	21	0	0	1	0	1
5	1	1	0	1	1	22	1	0	0	1	0
6	0	1	1	0	1	23	0	1	0	0	1
7	0	0	1	1	0	24	0	0	1	0	0
8	0	0	0	1	1	25	0	0	0	1	0
9	1	0	0	0	1	26	0	0	0	0	1
10	1	1	0	0	0	27	1	0	0	0	0
11	1	1	1	0	0	28	0	1	0	0	0
12	1	1	1	1	0	29	1	0	1	0	0
13	1	1	1	1	1	30	0	1	0	1	0
14	0	1	1	1	1	31	1	0	1	0	1
15	0	0	1	1	1	32	1	1	0	1	0
16	1	0	0	1	1	33	1	1	1	0	1

续表

i	a_5	a_4	a_3	a_2	a_1	i	a_5	a_4	a_3	a_2	a_1
34	0	1	1	1	0	37	0	1	1	0	1
35	1	0	1	1	1	38	0	0	1	1	0
36	1	1	0	1	1	39	0	0	0	1	1

从表 4-1 中可见 $i=31$ 时，状态恢复到 $i=1$ 的情况，该 LFSR 存在周期是 31，线性反馈寄存器中总假定 $c_1c_2\cdots c_n$ 中至少有一个系数不为 0，否则无论初始状态是什么，在最多 n 步后必然是 $00\cdots0$，而且一直维持此现状。

如果仅有一个系数，设 a_j 项系数不为零，则有

$$a_n(t=1)=a_j(t),\quad a_j(t=1)=a_{j+1}(t)。\quad i=1,2,\cdots,n-1$$

实际上是一个延迟装置。

引理 1：$c_n=1$ 的 n 级 LFSR，对于 a_i 的初值为 $0,i=1,2,\cdots,n$，其输出是周期序列。

若 a_i 不是全部为 $0,i=1,2,\cdots,n$，情况如何？

定义 4-1：若序列除开始若干项后的其余部分是周期序列，则称此序列为准周期序列。

如图 4-4 所示的 LFSR 输出序列是准周期序列，假定 r 是周期，m 是满足 $a_{m+t}=a_{m+r+t}$ 的最小正整数，t 是一切正整数，即 $a_m\neq a_{m+r}$；第 $m,m+1,m+r,m+r+1$ 时的状态分别是

$$a_m a_{m+1}\cdots a_{m+n+1}$$
$$a_{m+1}a_m\cdots a_{m+n}$$
$$a_{m+r}a_{m+r-1}\cdots a_{m+r+n-1}$$
$$a_{m+r+1}a_{m+r+2}\cdots a_{m+r+n}$$

由假设

$$a_{m+n}=c_na_m+c_{n-1}a_{m-1}+\cdots+c_1a_{m+n-1}$$
$$a_{m+n+r}=c_na_{m+r}+c_{n-1}a_{m+r+1}+\cdots+c_1a_{m+r+n-1}$$

但 $a_{m+n}=a_{m+r+n}$，从而 $c_na_m=c_na_{m+n}$，$c_n=1$，$a_m=a_{m+n}$ 与假设矛盾，故 $m=0$，即 $\{a_i\}$ 是周期序列。

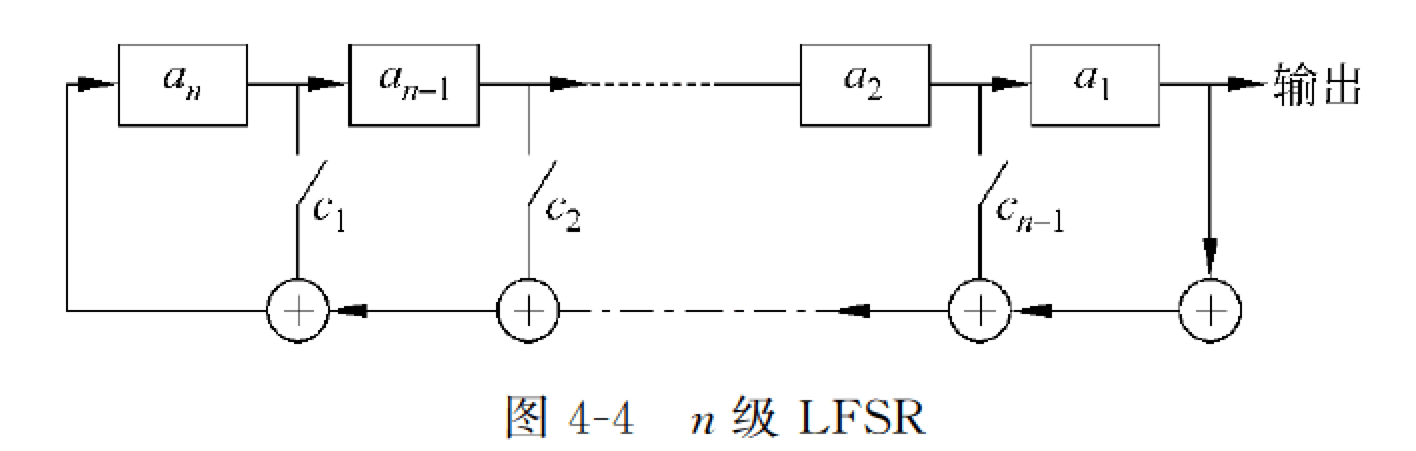


图 4-4　n 级 LFSR

引理 2：n 级 LFSR 对于 0 输入的输出是周期性的，其周期 $r\leqslant 2^n-1$。

证　根据引理 1，n 级 LFSR 对于零输入的输出是周期性的，若初始状态为 $a_n=a_{n-1}=\cdots=a_1=0$，则输出是 0。否则其状态就不会出现 $00\cdots0$，状态最多为 2^n-1，后一状态和前一状态由当前状态决定，而且是唯一决定，n 级 LFSR 的输出序列周期达到最大的 2^n-1。

4.3　Golomb 随机性概念

本节将讨论 LFSR 满足 Golomb 的随机性的三个公设。

G1：由线性移位寄存器结构相同时输出的序列也相同，所产生 m 序列的过程中必须遍历 2^n-1 个非零状态的每一个，然后才出现重复。这 2^n-1 个状态中 a_1 位有 2^n-1 个是 1，其余 2^n-1 个是 0，这就满足第一个公设。

G2：由于寄存器中不会出现全 0 状态，所以不会出现 0 的 n 游程，而且必然有一个 1 的 n 游程，但也不可能有长度更大的 1 游程。因为若出现 1 的 $n+1$ 游程，必然有两个 1 状态相邻，这是不可能的，1 的游程必出现在如下的串中：

$$0\underbrace{11\cdots1}_{n\text{位}}0$$

当这 $n+2$ 位通过 LFSR 时，依次出现

$$0\underbrace{1\cdots1}_{n-1\text{位}}\ \underbrace{1\cdots1}_{n\text{位}}\ \underbrace{1\cdots1}_{n-1\text{位}}0$$

所以不会出现 1 的 $n-1$ 游程，会出现 0 的 $n-1$ 游程：

$$1\underbrace{0\cdots0}_{n-1}1$$

它产生 $1\underbrace{0\cdots0}_{n-1}$ 和 $\underbrace{0\cdots0}_{n-1}1$ 两个状态。

如果 $n=2$，即 $n=2$ 级的 LFSR，满足 Golomb 公设。

如果 $n>2$，则 r 为不超过 $n-2$ 的任一正整数，任何 1 的 r 游程意味着存在串 $0\underbrace{1\cdots1}_{r}0$，为了计算 1 的 r 游程的数目，只要计算左边是这样的 $r+2$ 位的状态数目，任何一个 1 的 r 游程总会在通过 LFSR 时处在这样的位置，其余的 $n-r-1$ 位可以是由 0，1 构成的任何状态，所以 1 的 r 游程的数目为 2^{n-r-1}，于是在每一循环中出现 1 游程的数目为 $1+\sum_{r=1}^{n-2}2^{n-r+2}=2^{n-2}$；0 的游程数目也是 2^{n-2}。

小结：

(1) 任一循环含 2^{n-1} 个 1，$2^{n-1}-1$ 个 0。

(2) 1 的 n 游程有一个，没有 0 的 n 游程。

(3) 没有 1 的 $n-1$ 游程，有一个 0 的 $n-1$ 游程。

(4) 若 $1\leqslant r\leqslant n-2$，则 1 和 0 的 r 游程各 2^{n-r-1} 个。

(5) 每一循环有 2^{n-2} 个 1 的游程和 2^{n-2} 个 0 的游程。

G3：自相关函数 $c(t)$ 对于某整数 K，满足

$$nc(t)=\sum_{i=0}^{n-1}(2s_i-1)(2s_{i+t}-1)=\begin{cases}n, & t=0\\ K, & i\leqslant t\leqslant n-1\end{cases}$$

这个自相关函数 $c(t)$ 是用来度量序列 s 和 s 移位 t 位的相似性。

若 s 是随机的周期 N 序列，则 $|Nc(t)|$ 可能是非常小的 $(0<t<n)$。

例 4-1　周期 $n=15$，$s^{15}=0,1,1,0,0,1,0,0,0,1,1,1,1,0,1$，可证其满足 Golomb 随机公设。

(1) s^{15} 中 0 的数目为 7，1 的数目是 8。

(2) s^{15} 有 8 轮，有 4 轮只为 1，两轮为长度 2，一轮为长度 3，一轮长为 4。

(3) 自相关函数 $c(t)$ 有两个值：$c(0)=1$，$c(t)=\frac{1}{15}$，$1\leqslant t\leqslant 4$。

定理 4-1（换行定理）：周期为 2^n-1 的 m 序列，其异相自相关函数等于 $\frac{-1}{2^n-1}$。

证　设 $\{a_t\}$ 是周期为 2^n-1 的 m 序列，对正整数 τ，$0<\tau<2^n-1$，$\{a_t\}+\{a_{t+\tau}\}$ 在一个周期内为 0 的位的数目正好是序列 $\{a_t\}$ 和 $\{a_{t+\tau}\}$ 对应的位相同的位的数目，其中 $\{a_{t+\tau}\}$ 是将 $\{a_t\}$ 序列平行 τ 位而成。

设序列 $\{a_t\}$ 满足

$$a_{h+n}=c_1a_{h+n-1}+c_2a_{h+n-2}+\cdots+c_na_h$$

$$a_{h+n+\tau}=c_1a_{h+n+\tau-1}+c_2a_{h+n+\tau-2}+\cdots+c_na_{h+\tau}$$

$$a_{h+n}+a_{h+n+\tau}=c_1(a_{h+n-1}+a_{h+n+\tau-1})+c_2(a_{h+n-2}+a_{h+n+\tau-2})+\cdots+c_n(a_h+a_{h+\tau})$$

令 $b_j=a_j+a_{j+\tau}$ 故

$$b_{h+n}=c_1b_{h+n-1}+c_2b_{h+n-2}+\cdots+c_nb_h$$

$\{b_j\}$ 实际上也是 m 序列，为了计算 $R(\tau)$，只要将 $\{b_j\}$ 在某一循环中 0 的个数减去 1 的个数，再除以 2^n-1，即

$$R(\tau)=\frac{2^{n-1}-1-2^{n-1}}{2^n-1}=\frac{-1}{2^n-1}$$

4.4　非线性移位寄存器举例

先看一个 JK 触发器的例子。

如图 4-5 所示，LFSR1 是 m 级，$\{a\}$ 是它的输出，LFSR2 是 n 级，$\{b\}$ 是其输出，它的工作用表 4-2 表示。

图 4-5　JK 触发器

表 4-2　图 4-5 对应表

J	K	c_n
0	0	c_{n-1}
0	1	0
1	0	1
1	1	c_{n-1}

这种体制随机性方面较好，关系比较简单，容易从 $\{c_i\}$ 对 $\{a_i\}$，$\{b_j\}$ 作出推断。

这种体制的随机性比较好，然而只要知道序列的一部分便可推导出这些方程的解。

(1) 若 $c_n=c_{n-1}=0$，则 $a_{n+1}=0$。

(2) 若 $c_n=0, c_{n-1}=1$，则 $a_{n+1}=1$。

(3) 若 $c_n=1, c_{n+1}=0$，则 $b_{n+1}=1$。

(4) 若 $c_n=c_{n+1}=1$，则 $b_{n+1}=0$。

即从 c_n 和 c_{n+1} 便可对 a_{n+i} 和 b_{n+i} 中的 i 作出判定。故这个体制是非安全的。

例 4-2　LFSR1 $a_4(t+1)=a_2(t)+a_1(t)$　初态(11111)

　　　　LFSR2 $a_3(t+1)=a_2(t)+a_1(t)$　初态(1111)

由 LFSR1(见图 4-6)的输出和 LFSR2(见图 4-7)的输出的和构成输出列$\{c\}$，如表 4-3 所示。

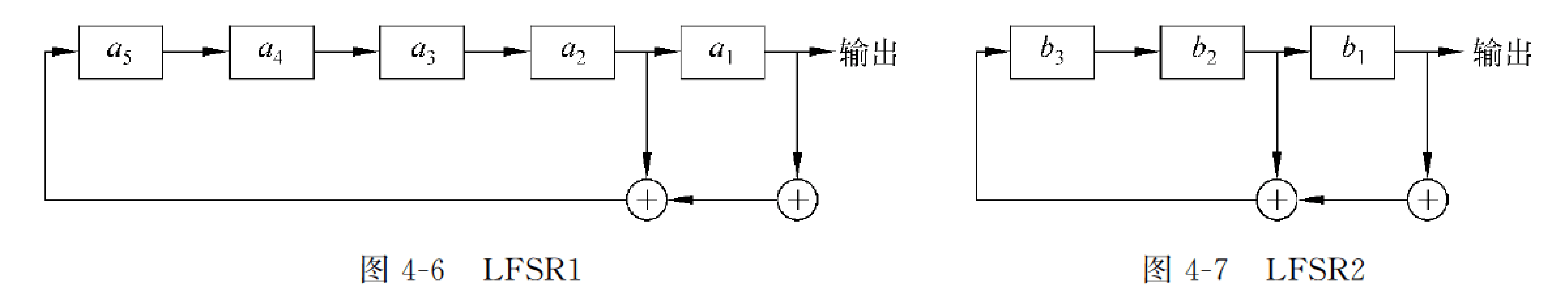


图 4-6　LFSR1　　　　图 4-7　LFSR2

表 4-3　输出列$\{c\}$

a_4	a_3	a_2	a_1		b_3	b_2	b_1		c		a_4	a_3	a_2	a_1		b_3	b_2	b_1		c
1	1	1	1		1	1	1		0		0	1	1	1		1	0	0		1
0	1	1	1		0	1	1		0		0	0	1	1		0	1	0		1
0	0	1	1		0	0	1		0		0	0	0	1		1	0	1		0
0	0	0	1		1	0	0		1		1	0	0	0		1	1	0		0
1	0	0	0		0	1	0		0		0	1	0	0		1	1	1		1
0	1	0	0		1	0	1		1		0	0	1	0		0	1	1		1
0	0	1	0		1	1	0		0		1	0	0	1		0	0	1		0
1	0	0	1		1	1	1		0		1	1	0	0		1	0	0		0
1	1	0	0		0	1	1		1		0	1	1	0		0	1	0		0
0	1	1	0		0	0	1		1		1	0	1	1		1	0	1		0
1	0	1	1		1	0	0		1		0	1	0	1		1	1	0		1
0	1	0	1		0	1	0		1		1	0	1	0		1	1	1		1
1	0	1	0		1	0	1		1		1	1	0	1		0	1	1		0
1	1	0	1		1	1	0		1		1	1	1	0		0	0	1		1
1	1	1	0		1	1	1		1		1	1	1	1		1	0	0		1
1	1	1	1		0	1	1		0		0	1	1	1		0	1	0		1
0	1	1	1		0	0	1		0		0	0	1	1		1	0	1		0
0	0	1	1		1	0	0		1		0	0	0	1		1	1	0		1
0	0	0	1		0	1	0		1		1	0	0	0		1	1	1		1

续表

a_4	a_3	a_2	a_1		b_3	b_2	b_1		c		a_4	a_3	a_2	a_1		b_3	b_2	b_1		c
1	0	0	0		1	0	1		1		0	1	0	0		0	1	1		1
0	1	0	0		1	1	0		0		0	0	1	0		0	0	1		1
0	0	1	0		1	1	1		1		1	0	0	1		1	0	0		1
1	0	0	1		0	1	1		0		1	1	0	0		0	1	0		0
1	1	0	0		0	0	1		1		1	0	1	1		1	1	0		1
0	1	1	0		1	0	0		0											
1	0	1	1		0	1	0		1		0	1	0	1		1	1	1		0
0	1	0	1		1	0	1		0		1	0	1	0		0	1	1		1
1	0	1	0		1	1	0		0		1	1	0	1		0	0	1		0
1	1	0	1		1	1	1		0		1	1	1	0		1	0	0		0
1	1	1	0		0	1	1		1		1	1	1	1		0	1	0		1
1	1	1	1		0	0	1		0		0	1	1	1		1	0	1		0

由表 4-3 可见序列$\{c\}$的周期扩大了。

例 4-3　Press 体制。

如图 4-8 所示的 Press 体制可以用来生成伪随机序列，它由 4 组 JK 触发器组成，还要加上循环计数器，用来决定每一个时间脉冲作用下输出的单元。

这个体制的密钥是 8 个移位寄存器的初态以及输出单元的顺序。

如图 4-9 所示有 LFSR A 和 LFSR B。LFSR A 输出是二进制地址，复合序列输出的正是根据 LFSR A 所指定的地址从 LFSR B 中取出的内容，具体见图 4-10。

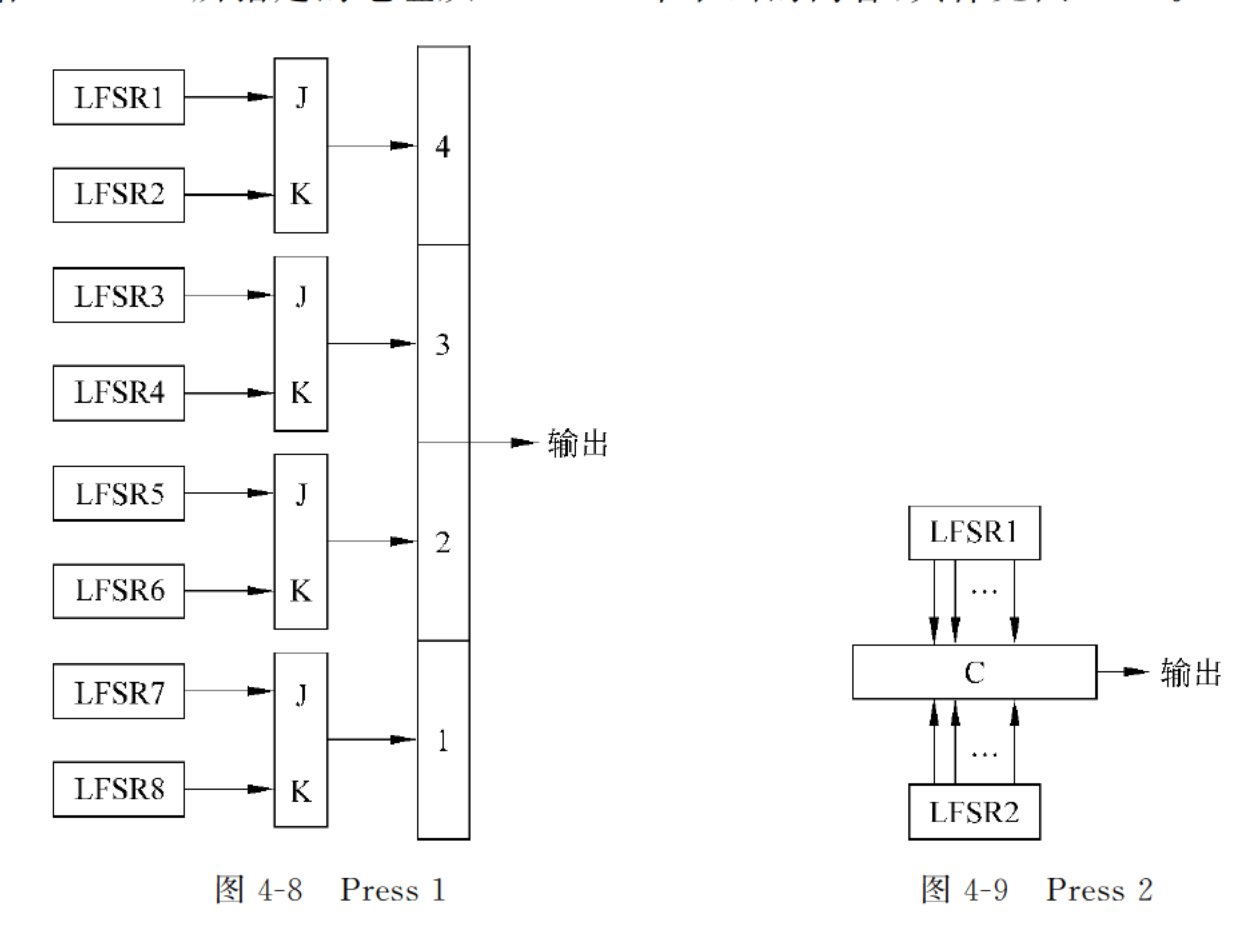


图 4-8　Press 1　　　图 4-9　Press 2

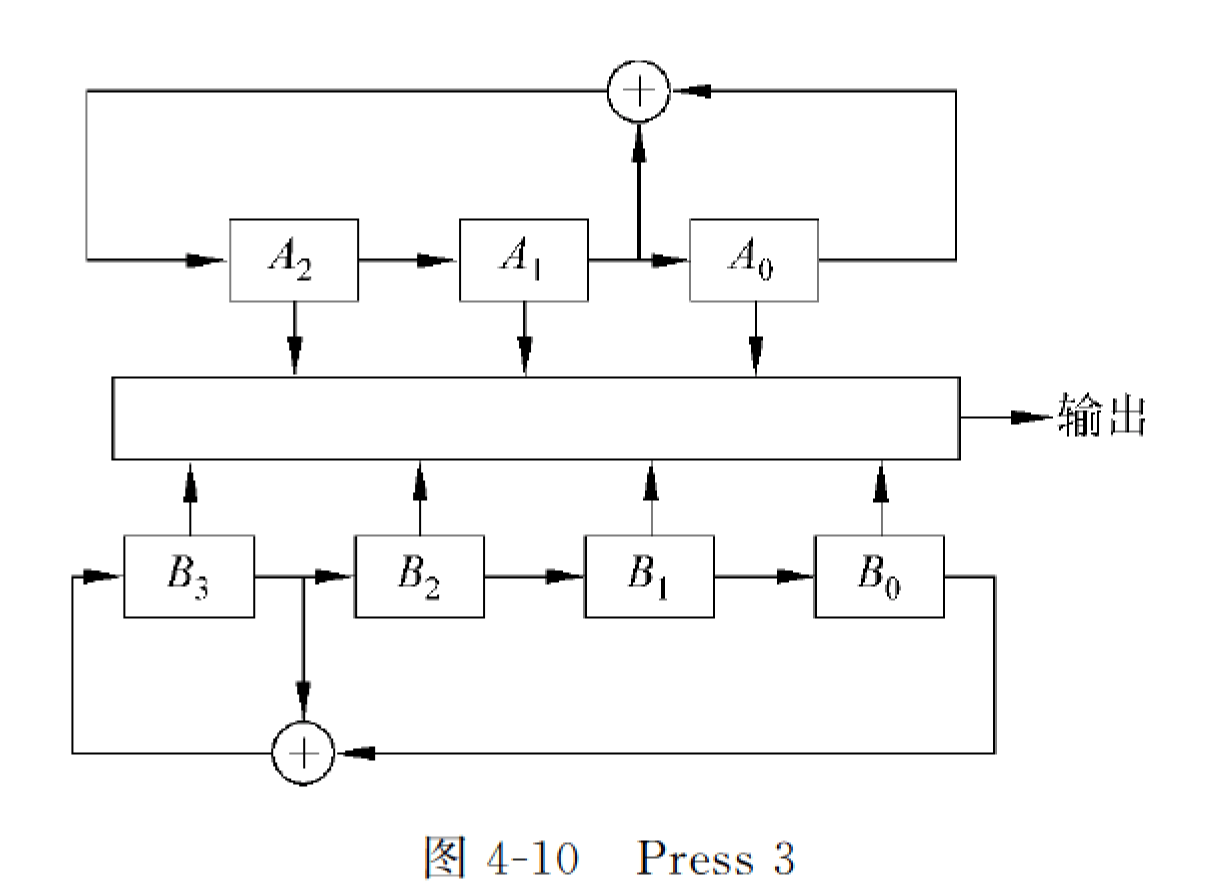


图 4-10　Press 3

复合序列的具体方案非常多。

例如：$A_i(i=1,2,3)$，$B_j(j=1,2,3,4)$，$\{A_i\}$，$\{B_j\}$ 可以加以重新编号。

设 $A_2A_1A_0$ 的初值为 011，$B_3B_2B_1B_0$ 的初值为 1000，复合序列输出是 B_N，$N=(A_2A_1)$，见表 4-4。

表 4-4　图 4-10 对应表

A_2	A_1	A_0	B_3	B_2	B_1	B_0	$N=(A_2A_1)$		B_N
1	1	1	1	0	0	0	1	1	1
0	1	1	1	1	0	0	0	1	0
0	0	1	1	1	1	0	0	0	0
1	0	0	1	1	1	1	1	0	1
0	1	0	0	1	1	1	0	1	1
1	0	1	1	0	1	1	1	0	0
1	1	0	0	1	0	1	1	1	0
1	1	1	1	0	1	0	1	1	1
0	1	1	1	1	0	1	0	1	0
0	0	1	0	1	1	0	0	0	0
1	0	0	0	0	1	1	1	0	0
0	1	0	1	0	0	1	0	1	0
1	0	1	0	1	0	0	1	0	1
1	1	0	0	0	1	0	1	1	0
1	1	1	0	0	0	1	1	1	0
0	1	1	1	0	0	0	0	1	0

复合序列是周期的，其周期 r 满足

$$r \leqslant (2^m - 1)(2^n - 1)$$

其中，m 是 LFSR A 的级数，n 是 LFSR B 的级数。

当$(m,n)=1$ 时 $r=(2^m-1)(2^n-1)$，一般有 $r=\text{lcm}\{2^m-1,2^n-1\}$。

4.5　LFSR 的密码反馈

密码反馈的基本特性是将密文反馈给系统，以进行后面的加密，下面先举一简单的例子。

m = cryptography is the science of data security

用维吉利亚密码加密，密钥是 redstar，过程如下。

m：cryptographyisthescienceofdatasecurity

k：redstarredstarredstarredstarredstarred

c：TVBHMOXIESZPIJKLHKUIVEGHGYDRKEVWDUIZXB

redstar 第一次结束时，紧接着用密文 TVBHMOX 进行加密。

m：cryptographyisthescienceofdatasecurity

k：redstarTVBHMOXKVQOKWPDCUGMGTQEYURJTJEQ

c：TVBHMOXKVQOKWPDCUGMGTQEYURJTJEQYTDKRJO

m：	cryptog	r	a	p	h	y	i	s
k：	redstar	$(r+T)$	$(e+V)$	$(d+B)$	$(s+H)$	$(t+M)$	$(a+O)$	$(r+X)$
c：	TVBHMOX	B	Z	T	G	D	W	G
t	h	e	s	c	i	e	n	c
$(r+B)$	$(e+Z)$	$(d+T)$	$(s+G)$	$(t+D)$	$(a+W)$	$(r+G)$	$(r+L)$	$(e+K)$
L	K	A	Q	Y	E	B	P	Q
e	o	f	d	a	t	a	s	e
$(d+A)$	$(s+Q)$	$(t+Y)$	$(a+E)$	$(r+B)$	$(r+P)$	$(e+Q)$	$(d+H)$	$(s+W)$
H	W	W	H	S	Z	U	C	S
c	u	r	i	t	y			
$(t+W)$	$(a+H)$	$(r+S)$	$(r+Z)$	$(e+O)$	$(d+C)$			
R	B	A	Y	R	D			

图 4-11 是利用 LFSR 进行密码反馈的示意图。

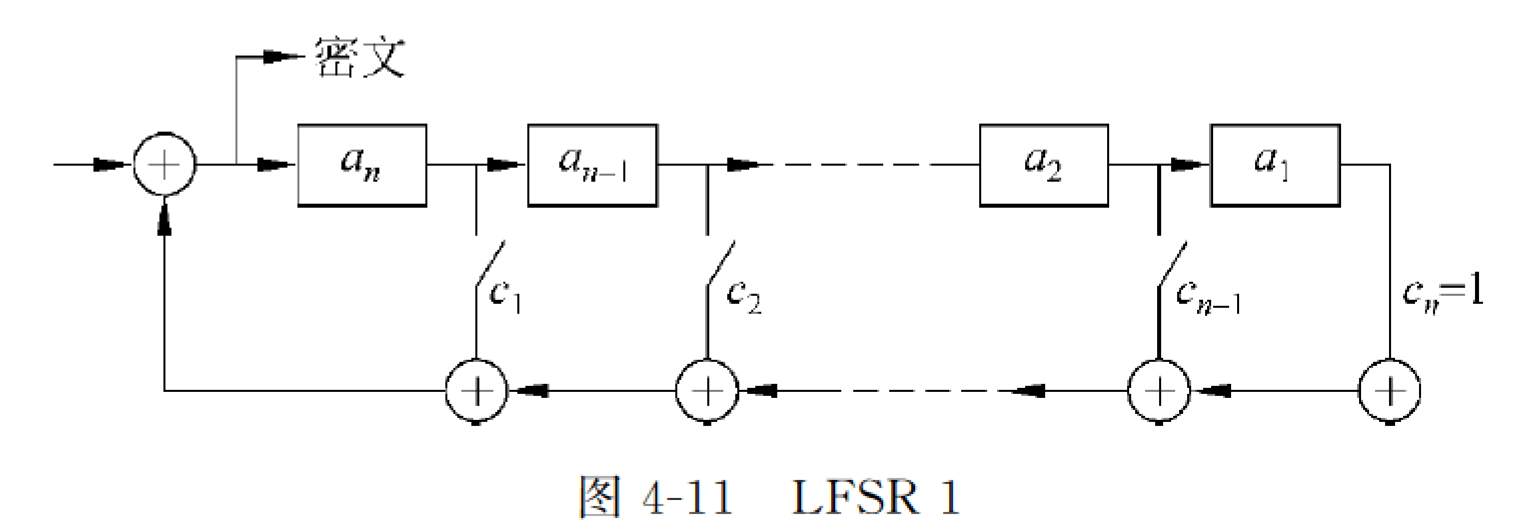


图 4-11　LFSR 1

密钥：$c_1,c_2,\cdots,c_n,a_1,a_2,\cdots,a_n$的初态 $s_1,s_2,\cdots,s_n$

明文 $m=m_1m_2\cdots$

密文 $c=e_1e_2\cdots$

$$e_1 = m_1 + \sum_{i=1}^{n} c_i s_{n-i+1}$$

$$e_2 = m_2 + \sum_{i=2}^{n} c_i s_{n-i+2} + c_1 e_1$$

$$e_3 = m_3 + \sum_{i=3}^{n} c_i s_{n-i+3} + c_1 e_2 + c_2 e_1$$

$$\cdots$$

$$e_k = m_k + \sum_{i=k}^{n} c_i s_{n-i+k} + \sum_{i=1}^{k-1} c_i e_{k-i}$$

$$e_{n+1} = m_{n+1} + \sum_{i=1}^{n} c_{n-i+1}$$

$$\cdots$$

$$e_{n+h} = m_{n+h} + \sum_{i=1}^{n} c_{n-i+h}$$

又如图 4-12 所示,移位寄存器的初态为 $S_1,S_2,\cdots,S_n$,系数是 $c_1,c_2,\cdots,c_n$时都与加密的 LFSR 相同,即解密密钥与加密密钥相同。这样当输入密文 $c_1c_2\cdots c_n$时便输出明文 $m=m_1m_2\cdots m_n$,实现了解密。

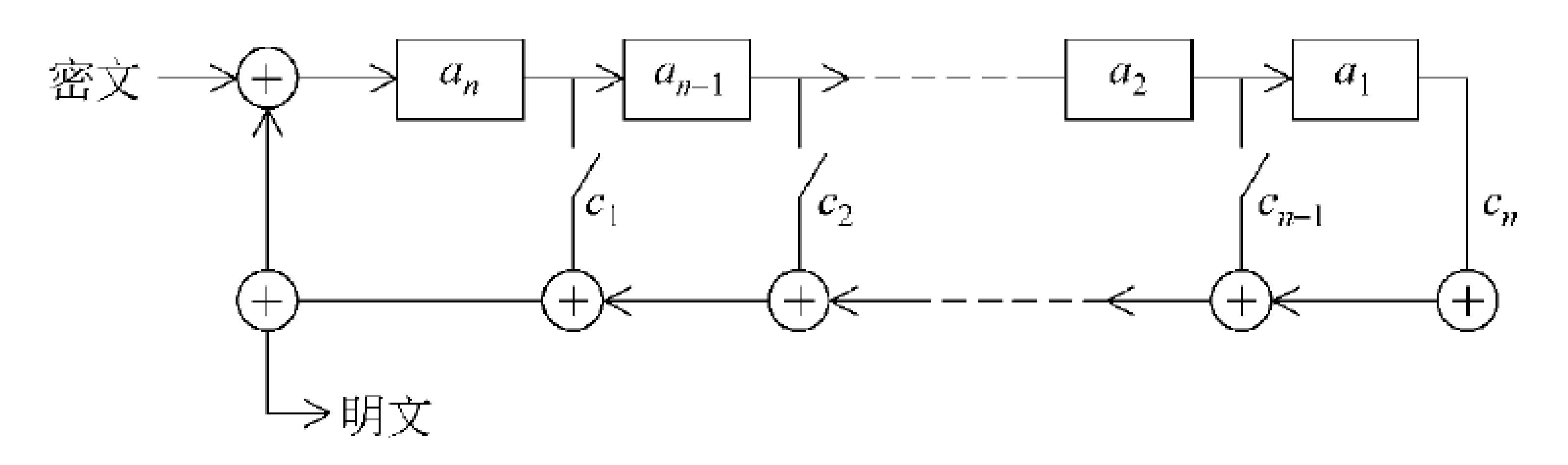
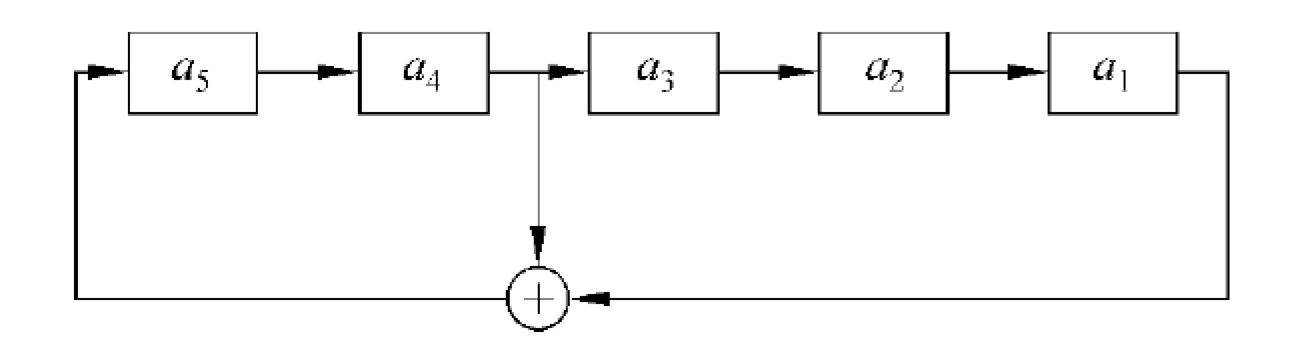


图 4-12　LFSR 2

习　　题

如果 $t=0$ 时,$a_1a_2a_3a_4a_5$ 初态为 10101,求上述移位寄存器各个时间的状态。



第 5 章　判定素数的算法

5.1　数 学 准 备

1. 定义 Fermat 伪素数

定义 5-1：n 是奇合数，a 是一整数，$1 \leqslant a \leqslant -1$，若 $a^{n-1} \equiv 1 (\bmod\ n)$，则称 n 是关于 a 的伪素数。

由 Fermat 定理可知，若 p 是素数，a 是一整数，$p \nmid a$，则 $a^{p-1} \equiv 1 (\bmod\ p)$。

例 5-1　$n=341$，$2^{340} \equiv 1 (\bmod\ 341)$，但 $341=31\times 11$ 不是素数。

2. 定义 Carmichael 数

定义 5-2：合数 n，对所有正整数 b，满足 $(b,n)=1$，$b^{n-1} \equiv 1 (\bmod\ n)$ 都成立，则称 n 为 Carmichael 数。

例 5-2　$561=3\times 11\times 17$ 是 Carmichael 数。

$(b,561) \equiv 1$，$(\bmod\ 561)$，则 $(b,3)=(b,11)=(b,17)=1$。

由 Fermat 定理，$b^2 \equiv 1 (\bmod\ 3)$，$b^{10} \equiv 1 (\bmod\ 11)$，$b^{16} \equiv 1 (\bmod\ 17)$。

所以

$$b^{560} \equiv 1 (\bmod\ 3), \quad b^{560} \equiv 1 (\bmod\ 11), \quad b^{560} \equiv 1 (\bmod\ 17),$$

$$b^{560} \equiv 1 (\bmod\ 561), \quad (b,561) = 1$$

Carmichael 数有无穷多个。

定义 5-3：$S \geqslant 2$，整数，形为 2^S-1 的素数称为 Mersenne 素数。

3. 求 $a^k \bmod n$ 的算法

S1 分解 $k = (k_t k_{t-1} \cdots k_1 k_0)_2 = \sum_{i=0}^{t} k_i 2^{k_i}$。

S2 $b \leftarrow 1$，若 $k=0$ 则输出 (b)。

S3 $A \leftarrow a$。

S4 若 $i \leqslant t$ 则作

　始 $A \leftarrow A^2 (\bmod\ n)$，

　　若 $k_i=1$ 则作**始** $b \leftarrow A \cdot b (\bmod\ n)$**终** 否则

　始 $i \leftarrow i+1$，转 S4 **终 终**。

S5 输出 (b)。

4. 求雅科比符号 $\left(\dfrac{a}{n}\right)$ 的算法

$n \geqslant 3$ 整数，$0 \leqslant a < n$。

S1 若 $a=0$，则输出(0)。

S2 若 $a=1$，则输出(1)。

S3 若 $a=2^e a_1$，a_1是奇数。

若 e 是偶数则令 $S\leftarrow 1$，否则作：若 $n\equiv 1 \pmod 8$ 或 $n\equiv 7 \pmod 8$，则 $S\leftarrow 1$；若 $n\equiv 3 \pmod 8$，或 $n\equiv 5 \pmod 8$，则 $S\leftarrow -1$。

S4 若 $n\equiv 3 \pmod 4$ 和 $a_1\equiv 3 \pmod 4$，则作 $S\leftarrow -S$。

S6 $n_1\leftarrow n \pmod{a_1}$。

S8 若 $a_1=1$，则输出(S)，否则输出$\left(S\cdot\left(\frac{a_1}{n_1}\right)\right)$。

5. 雅科比符号的性质

(1) $\left(\frac{a}{n}\right)=0,1$ 或 -1，$\left(\frac{a}{n}\right)=0$，当且仅当 $\gcd(a,n)\neq 1$。

(2) $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$，若 $a\in Z_n^*$，则$\left(\frac{a^2}{n}\right)=1$。

(3) $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$。

(4) 若 $a\equiv b, \pmod n$ 则$\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$。

(5) $\left(\frac{1}{n}\right)=1$。

(6) $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$，所以$\left(\frac{-1}{n}\right)=1$，若 $n\equiv 1 \pmod 4$。

(7) $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$，故若 $n\equiv 1 \pmod 8$或 $n\equiv 7 \pmod 8$，则$\left(\frac{2}{n}\right)=1$。

$n\equiv 3 \pmod 8$或 $n\equiv 5 \pmod 8$，则$\left(\frac{2}{n}\right)=-1$。

(8) $\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$，即$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)$，除非 m 和 n 是 $m\equiv 3 \pmod 4$，$n\equiv 3 \pmod 4$。

6. 欧拉准则

n 是奇合数，a 是 $1\leqslant a\leqslant n-1$ 的整数，若 $\gcd(a,n)>1$ 或 $a^{\frac{n-1}{2}}\not\equiv\left(\frac{a}{n}\right)\bmod n$，则称 a 对 n 是合数。

反过来，即 $\gcd(a,n)=1$，$a^{\frac{n-1}{2}}\equiv\left(\frac{a}{n}\right)\bmod n$，则称 a 是欧拉伪素数。

欧拉准则可以作为素数判定依据在于 n 是奇合数。

例 5-3　合数 $91=7\times 13$，关于 9 是欧拉伪素数。

$$9^{45}\equiv 1 \pmod{91},\quad \left(\frac{9}{91}\right)=1$$

欧拉准则可以作为素数的概率判定的依据在于：n 是奇合数，$1\leqslant a\leqslant n-1$ 的所有数 a，最多 $\frac{1}{2}\Phi(n)$，是基于欧拉判定 n 是伪素数。

5.2 概率算法

下面介绍概率算法，从一个生日问题的例子来说明。

问题是这样的，试问有多少人在一起，使其中至少有两人的生日相同的概率为 $\frac{1}{2}$？

有一对生日相同的概率等于 1 减去两人生日不相同的概率。令 p_m 表示 m 个人在一起，存在相同生日的概率。

$$p_1=1,\quad p_2=1-\frac{364}{365}=\frac{1}{365},\quad p_3=\left(1-\frac{4}{365}\right)\left(1-\frac{363}{365}\right)=\frac{1}{365}\times\frac{2}{365}$$

可得递推关系：

$$p_m=\frac{365-(m-1)}{365}p_{m-1}$$

$$p_1=1$$

$$p_2=\left(1-\frac{1}{365}\right)$$

$$p_3=\left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)$$

$$p_4=\left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\left(1-\frac{3}{365}\right)$$

$$\cdots$$

$$p_m=\left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\cdots\left(1-\frac{m-1}{365}\right)$$

根据

$$\mathrm{e}^x=1+x+\frac{1}{2!}x^2+\frac{1}{3!}x^3+\cdots\geqslant 1+x$$

故

$$p_m\leqslant \mathrm{e}^{-\frac{1}{365}}\mathrm{e}^{-\frac{2}{365}}\cdot\cdots\cdot\mathrm{e}^{-\frac{m-1}{365}}=\mathrm{e}^{-\sum_{i=1}^{m-1}\frac{p}{365}}$$

$$p_m\leqslant \mathrm{e}^{-\frac{1}{365}(1+2+\cdots+\overline{m-1})}=\mathrm{e}^{-\frac{1}{365}\times\frac{1}{2}m(m-1)}$$

若 $\mathrm{e}^{-\frac{1}{365}\times\frac{1}{2}m(m-1)}\leqslant\frac{1}{2}$，即 p_m 为存在一对生日相同的概率超过或等于 $\frac{1}{2}$。

$m\geqslant 23$，说明 23 人中有 $\frac{1}{2}$ 的概率其中至少有两人生日相同。

若将问题改为多少人在一起使得至少有一人和其中某一人 A 有相同的生日的概率超过 $\frac{1}{2}$，令 q_m 表示 m 个人在一起至少有一人和 A 有相同的生日的概率超过 $\frac{1}{2}$，令 q_m 表

示 m 个人在一起至少有一人和 A 有相同的生日的概率，则

$$q_1 = \frac{364}{365}, \quad q_2 = \left(\frac{364}{365}\right)^2, \quad \cdots, \quad q_m = \left(\frac{364}{365}\right)^m$$

若

$$\left(\frac{364}{365}\right)^m \leqslant \frac{1}{2}, \quad m\log\frac{364}{365} \leqslant -\log 2$$

$$m \geqslant \frac{-\log 2}{\log\left(\frac{364}{365}\right)} > 253$$

这说明只有超过 253 个人在一起，才使得无一人生日与 A 都不同的概率$\leqslant\frac{1}{2}$，换而言之，至少有一人与 A 生日相同的概率超过$\frac{1}{2}$。

5.3 随机数的发生器

1. 线性同余式法

概率算法需要随机数，下面介绍伪随机数的产生，真正的随机数是不可能利用计算机产生的。

最简单的伪随机数可通过线性同余式得到，即

$$a_{n+1} = ba_n + c \bmod n, \quad a_0 = d$$

其中，$b\geqslant 0$，$c\geqslant 0$，$d\leqslant p$，d 称为种子，取 p 为大素数，而且 b、$c<p$，因 b、c、m 给定后，d 不同将产生不同的伪随机数序列，因此产生的伪随机数序列比较均匀。

例 5-4 $p=23$，$b=2$，$d=5$，$a_0=5$。

$$a_1 \equiv 2\times 5+3, \quad \bmod 23 \equiv 13$$
$$a_2 \equiv 2\times 13+3, \quad \bmod 23 \equiv 6$$
$$a_3 \equiv 2\times 6+3, \quad \bmod 23 \equiv 15$$
$$a_4 \equiv 2\times 15+3, \quad \bmod 23 \equiv 10$$
$$a_5 \equiv 2\times 15+3, \quad \bmod 23 \equiv 0$$
$$a_6 \equiv 3$$
$$a_7 \equiv 2\times 3+3, \quad \bmod 23 \equiv 9$$
$$a_8 \equiv 2\times 9+3, \quad \bmod 23 \equiv 21$$
$$a_9 \equiv 2\times 21+3, \quad \bmod 23 \equiv 22$$
$$a_{10} \equiv 2\times 22+3, \quad \bmod 23 \equiv 1$$
$$a_{11} \equiv 2\times 1+3, \quad \bmod 23 \equiv 5$$
$$a_{12} \equiv 2\times 5+3, \quad \bmod 23 \equiv 13$$
$$\cdots$$

故得随机序列 13，6，15，10，0，3，9，21，22，1，5，13，…

2. 离散对数法

假定 p 是一大素数，a_0 是一常数，q 也是常数，满足

$$\gcd(q, p-1) = 1$$

令 $a_{n+1} \equiv a_n^q$，mod p，$n=0,1,2,\cdots,n$；由此产生一伪随机序列：$a_0, a_1, a_2, \cdots, a_n$；条件 $\gcd(q, p-1)=1$，由 Fermat 定理，因 $a^{p-1} \equiv 1$，mod p，结果导致 $a_{n+1} \equiv a_{n+2} \equiv \cdots \equiv 1$。

例 5-5　$p=17$，$a_0=3$，$q=2$。

$$a_1 \equiv 3^2 \bmod 17 \equiv 9$$

$$a_2 \equiv 9^2 \bmod 17 \equiv 81 \bmod 17 \equiv 13$$

$$a_3 \equiv 13^2 \bmod 17 \equiv 16$$

$$a_4 \equiv 16^2 \bmod 17 \equiv 256 \bmod 17 \equiv 1$$

由于 $p=17$ 太小，故周期也太短。

3. 素数法

假定 p 是一大素数，$\frac{1}{p}$ 是一小数，小数点后第一个非空数开始为伪随机数序列。

例如 $p=19$，$\frac{1}{19}=0.052\,631\,578\,947\,368\,421\,005\,263\,15\cdots$ 伪随机数序列为 5，2，6，3，1，5，7，8，9，4，7，3，6，8，4，2，1，周期达到 17。

4. 素数判定的若干定理

1）关于素数的若干定理

素数的分布非常稀疏，而且随着数位的增多而更加稀疏。

设 $\pi(x)$ 为小于或等于 x 的全部素数个数，则 $\lim\limits_{a\to\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1$，即 $\pi(x)=\frac{x}{\ln x}$，见表 5-1。

表 5-1　素数数目表

n	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9
$\pi(n)$	4	2.5	165	1229	9592	78 498	664 579	5 761 455	50 847 534

以 $\frac{10^9}{\ln 10^9} \approx 48\,254\,942$，$50\,847\,534-48\,254\,942=259\,259$ 与 10^9 的比约为 0.0026。

一般可证 n 位十进制数中素数的密度约为 $\frac{1}{n\ln 10}$，可见其稀疏性。

和素数有关的定理有 Wilson 定理和 Fermat 定理。

定理（Wilson）：n 是素数的充分条件为 $(n-1)! \equiv -1 \bmod n$。

证　必要性：

n 是素数，所以对 $\{1,2,\cdots,n-1\}$ 中的每一个数 a，必存在 a^{-1} 使 $aa^{-1}=a^{-1}a=1 \bmod n$。其中，1 的逆元素为 1，$(n-1)$ 的逆元素为 $n-1$，即 $1\times 1\equiv \bmod n$，$(n-1)(n-1)\equiv 1 \bmod n$。

除了 1 和$(n-1)$外，其余 $n-3$ 个数 $a\neq a^{-1}$，所以$(n-1)!\equiv(n-1)\equiv-1 \bmod n$。

充分性：

设$(n-1)!\equiv-1 \bmod n$，但 n 不是素数，则令 $n=ab$，$a>1$，$b>1$，则 $n\mid(n-1)!$，同时 $a\mid[(n-1)!+1]$，$a\mid[(n-1)!+1-(n-1)!]$，与 $a>1$ 矛盾。充分性得证。

Wilson 定理是素数的充要条件，但 n 十分大时，计算复杂度极高。

Fermat 定理：若 p 是素数，则对于任意整数 a，$\gcd(a,p)=1$ 应有 $a^{p-1}\equiv1 \bmod p$。

计算 a^n 无须 n 次乘法，仅需$\lfloor\log_2 n\rfloor$次乘法。Fermat 定理是判定素数的必要并不充分条件，即满足 $a^{n-1}\equiv1 \bmod n$，n 可能不是素数。

2）Solovay-Strassen 素数的概率测试法

输入奇数 $n>3$：

S1 将$\frac{1}{2}(n-1)$化成二进制数$\frac{n-1}{2}=(k_tk_{t-1}\cdots k_1k_0)_2$，$i\leftarrow1$。

S2 若 $i\leqslant t$，则作

始　选一随机数 a，$2\leqslant a\leqslant n-2$，计算 $r\equiv a^{\frac{n-1}{2}}(\bmod n)$。

若 $r\neq1$，$r\neq n-1$ 则作 **始** 输出“合数”，转 S2 **终**

计算 Jacobi 数 $S=\left(\frac{a}{n}\right)$，若 $r\not\equiv S \bmod n$ 则作

始 输出“合数”，转 S2 **终**

终，否则作

始 $i\leftarrow i+1$，转 S2 **终**。

S3 输出“素数”。

n 是合数，而 Solovay-Strassen 算法给出“素数”的概率$<\left(\frac{1}{2}\right)^t$。

若 $\gcd(a,n)=d$，则 $d=a^{\frac{n-1}{2}} \bmod n$ 即因子，所以 $r\neq1$ 省去测试 $\gcd(a,n)\neq1$ 的必要条件，算法省去输出“合数”。

5.4　Miller-Rabin 测试法

输入一奇整数 $n>3$，输出“素数”或“合数”。

S1 $n-1=2^sr$，r 是奇数，$r=(r_tr_{t-1}\cdots r_0)_2$，$i\leftarrow1$。

S2 若 $i\leqslant t$，则作

始 选一随机数 a，$2\leqslant a\leqslant n-2$，计算 $a^r(\bmod n)$。

① 若 $y\neq1$ 和 $y\neq n-1$ 则作

始 $j\leftarrow1$

② 若 $j\leqslant s-1$ 和 $y\neq n-1$ 则作

始 计算 $y\leftarrow y^2(\bmod n)$

若 $y=1$ 则作 **始** 输出“合数”，转②，

终。

$j\leftarrow j+1$，转②。

终。

若 $y \neq n-1$ 则作**始** 输出"合数",转①**终**

终

$i \leftarrow i+1$,转 S2

终

S3 输出(素数)

事实上,令 n 是奇素数,$n-1=2^s r$,r 是奇数,a 是满足 $\gcd(a,n)=1$ 的任意整数,则 $a^r \equiv 1 \pmod n$ 或 $a^{2^j r} \equiv -1 \pmod n$,$0 \leqslant j \leqslant s-1$。

定义 5-4：a 是一奇合数,$n-1=2^s r$,r 是奇数,a 是$[1,n-1]$区间上的数：

① 若 $a^r \not\equiv 1 \pmod n$ 和 $a^{2^j r} \not\equiv -1 \pmod n$,$0 \leqslant j \leqslant s-1$,则 a 称为 n 的合数的强证明。

② 反之若 $a^r \equiv 1 \pmod n$或 $a^{2^j r} \equiv -1 \pmod n$,$0 \leqslant j \leqslant s-1$,则称 n 关于 a 为强伪素数。

例 5-6　$n=91=7\times 13$,$91-1=90=2\times 45$,$s=1$,$r=45$,$9^r=9^{45}\equiv 1 \pmod{91}$,91 关于 9 是强伪素数,91 关于$\{1,9,10,12,16,17,22,29,38,53,62,69,74,75,79,81,82,90\}$中的数是强伪素数。

Miller-Rabin 算法和 Solovay-Strassen 算法的比较：

(1) Solovay-Strassen 计算量比较大;

(2) Solovay-Strassen 法比较难于实验,包括雅科比符号的计算;

(3) Solovay-Strassen 法出错的概率为 $\left(\frac{1}{2}\right)^t$,Miller-Rabin 出错的概率为 $\left(\frac{1}{4}\right)^t$。

5.5　Miller-Rabin 算法的有关定理

定理 5-1　若 $n>4$ 是合数,n 的适合于合数的 b 的数目大于或等于$\frac{3}{4}(n-1)$。

证　从略。

(1) 素数的生成,令 $p(N)$ 表$\{2,3,\cdots,N\}$ 的素数数目,$p(N)\sim\frac{N}{\log N}$,故最多 l 比特的素数数目为大约$\frac{2^l}{l\log 2}$,这说明 l 比特数是素数的概率是 $\Omega\left(\frac{1}{l}\right)$。

(2) 强素数：一素数 p 称为强素数,若存在整数 r,s,t 使之满足：

① $p-1$ 有大素数因子 r;

② $p+1$ 有大素数因子 s;

③ $r+1$ 有大素数因子 t。

5.6　附录 AKS 确定型判定素数的多项式算法

判定素数是密码学重要而热门的问题,相当一段时间里只限于概率算法,已见于本章前面的 Miller 概率测试法,直到 2002 年印度的三位科学家 M. Agrawal、N. Kayal、N. Saxena 发表一篇 *Primer is in P* 的论文,也就是"判定素数的多项式算法"。这一节的介绍是根据它的 2004 年的修改本,虽然结果离实用还有一段距离,但毕竟迈出了确定型多项式算法的步子,也许前面还有可资发展的空间。

引理　若 $a\in\mathbf{Z},n\in\mathbf{N},n\geqslant 2,\gcd(a,n)=1$，$n$ 是素数的充要条件是

$$(X+a)^n \equiv X^n + a \pmod n \tag{1}$$

证　对于 $0<i<n$，在 $((X+a)^n-(X^n+a))$ 中 x^i 项系数为 $\binom{n}{i}a^{n-i}$。若 n 是素数，则 $\binom{n}{i}\equiv 0 \pmod n$，所以 x^i 项系数为 0。

如果 n 是合数，q 是 n 的一个因数，令 $q^k \mid n, q^k \nmid \binom{n}{q}$ 且与 a^{n-q} 项系数互素，dmegX^q 项系数(mod n) 不为 0，则 $((X+a)^n-(X^n+a))$ 在 $\mathbf{Z}^n$ 不恒等于 0，证毕。

上面同余式提出了素数的一个简单测试：输入 n，选一 a 检测(1)是否满足，由于必须计算左端 n 项系数，在最坏情况下是 $\Omega(n)$ 的复杂度。

若取代(1)的是

$$(X+a)^n \equiv X^n + a \pmod{x^r-1,n} \tag{2}$$

由本节前面引理可知素数 n 满足(2)，对所有的 a 及合适小的 r，只要 n 是某些合数时，也有一些 a 和 r 满足(2)。

例如求 $(x+5)^{13} \pmod{13,x^3-1}$。

$$
\begin{aligned}
(x+5)^2 &\equiv x^2+10x+25 \equiv x^2-3x-1\\
(x+5)^3 &\equiv (x^2-3x-1)(x+5) \equiv x^3+2x^2-16x-5\\
&\equiv 2x^2-16x+(1-5) \equiv 2x^2-3x-4\\
(x+5)^6 &\equiv (2x^2-3x-4)^2 \equiv 4x^4-12x^3-7x^2+24x+16\\
&\equiv -7x^2+(4+24)x+(-12+16) \equiv 6x^2+2x+4\\
(x+5)^{12} &\equiv (6x^2+2x+4)^2 \equiv 36x^4+24x^3+52x^2+16x+16\\
&\equiv 10x^4+11x^3+3x+3 \equiv 1
\end{aligned}
$$

故 $(x+5)^{13}\equiv x+5$。

另一方面：

$$(x+2)^{65} \equiv 2x^6+2x^5+53x^4+49x^3+14x^2+52x+6 \pmod{65,x^7-1} \not\equiv x^{65}+2,$$

$$x^{65}+2 \equiv x^2\,(x^7)^9+2 \equiv x^2+2$$

65 不是素数，但

$$(x+5)^{1729} \equiv x^{1729}+5 \pmod{(1729,x^3-1)}$$

虽然 $(x+a)^{1729}\equiv x^{1729}+a \pmod{(1729,x^3-1)}$，但 $1729=7\times 13\times 19$ 是合数，而且

$$(x+5)^{1729} \equiv 1254x^4+799x^3+556x^2+106x+1520 \pmod{(1729,x^5-1)} \equiv x^4+5$$

但无论如何，适当地选择 r 和 a，使 $(X+a)^n\equiv X^n+a \pmod{x^r-1,n}$ 成立可在多项式时间内完成。

5.7　符号与准备

P 类：多项式类问题集合，是指计算机能在问题规模(设为 n)的多项式时间内完成的问题集合。

$Z_n=\{0,1,2,\cdots,n\}$关于 mod n 的加法成交换群，$Z_n\backslash\{0\}$ 关于 mod n 的乘法构成交换群，且分配律成立。

Z_n^*：与 n 互素的整数关于 mod n 的乘法构成的群。

$F_p=\{0,1,\cdots,p-1\}$，关于 mod p 的加法和乘法构成的域。

$\frac{F_p[x]}{(h(x))}$：设 $h(x)$ 是 d 次方不可化约的多项式，$\frac{F_p[x]}{(h(x))}$ 为阶为 p^d次方的有限域，即 mod $h(x)$ 的同余类。

$O^{\sim}(t(n))$ 是 $O(t(n)\cdot poly(\log t(n)))$，$O(f)\triangleq\{g:N\to R'\mid\exists c\in\mathbf{R}^+,\exists n_0\in\mathbf{N},\forall n\geqslant 0$，使 $g(n)\leqslant cf(n)\}$，其中 log 不加说明均以 2 为底。

$O_r(a)$表示 $a^k\equiv 1(\bmod r)$成立的 k 的最小正数。

引理 LCM(m)表示前面 m 个数的 lcm，$m\geqslant 7$ 时有 LCM(m)$\geqslant 2^m$。这个不等式的证明见附录 A。

5.8 AKS 算 法

输入整数 $n>1$。

S1 若($n=a^b,a\in\mathbf{N},b>1$) 则输出“合数”。

S2 找最小的 r，使 $O_r(n)>\log^2 n$。

S3 若 $1<(a,n)<n,a\leqslant r$，则输出“合数”。

S4 若 $n\leqslant r$，则输出“素数”，$a\leftarrow 1$。

S5 若 $a\leqslant\lfloor\sqrt{\Phi(r)}\log n\rfloor$则

始 若$(X+a)^n\not\equiv X^n+a\ (\bmod\ (x^r-1,n))$则**始** 输出“合数”，**终**

终 否则 **始** $a\leftarrow a+1$，转 S5 **终**。

S6 输出“素数”。

5.9 正确性证明

定理 5-2：算法输出“素数”当且仅当 n 是素数。

定理 5-2 是通过如下 7 个引理来证明的。

引理 1 若 n 是素数，算法输出是“素数”。

证 若 n 是素数，则 S1 和 S3 不输出“合数”，根据 5.4 节的引理 S3 也不会输出“合数”，所以算法确定素数与 S4 及 S5。

上面引理的逆要多花一些工夫，S4 输出“素数”，则 n 必须是素数，否则 S3 将找到 n 的一个非平凡因子，所以余下的情况是 S6 输出“素数”。算法的确定素数依据为 S4 和 S5。

引理 1 的逆：S4 输出“素数”，则 n 必须是素数，否则 S3 将找到 n 的非平度凡因子，所以余下的情况在 S6 输出“素数”。算法的主要步骤是 S2 和 S5。S2 找一合适的 r，S5 证明方程(2)对一些 a 是满足的。

引理 2 存在一个 $r\leqslant\max\{3,\lceil\log^5 n\rceil\}$，使 $O_r(n)>\log^2 n$。

证 $n=2, r=3$ 时明显引理为真，满足所有的条件。

假定 $n>2$，则$\lceil \log^5 n \rceil>10$，令 $r_1, r_2, \cdots, r_t$ 是所有 $O_{r_i}(n)\leqslant \log^2 n$ 或是 $r_i \mid n$，则每个 r_i除尽 $n \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor}(n^i-1)<n^{\log^4 n}\leqslant 2^{\log^5 n}$。

由 5.5 节的引理，前面$\lceil \log^5 n \rceil$这些数的 $l.c.m.$ 至少是 $2^{\lceil \log^5 n \rceil}$，故至少存在一数 $S\leqslant \lceil \log^5 n \rceil$，使 $S\notin\{r_1, r_2, \cdots, r_t\}$，若$(S,n)=1$，则 $O_S(n)>\log^2 n$，我们已做了的，若$(S,n)>1$，则因 S 不能除尽 n，$(S,n)\in\{r_1, r_2, \cdots, r_t\}$，$r=\dfrac{S}{(S,n)}\notin\{r_1, r_2, \cdots, r_t\}$，所以 $O_r(n)>\log^2 n$。证毕。

因 $O_r(n)>1$，则 n 必存在一素因子 p，使 $O_r(p)>1$，有 $p>r$；否则，因$(n,r)=1$，S3 或 S4 将确定素性，故有$[f(x)]^{mm'}\equiv f(x^{mm'})$，$(\bmod\ (x^r-1, p))$，证毕。

定义 5-5：性质(I)若$[f(x)-g(x)]^m\equiv[f(x)]^m[g(x)]^m\equiv f(x^m)g(x^m)(\bmod\ (x^r-1, p))$，则称 $f(x)\cdot g(x)$具有性质(I)。

上面两个引理说明集合 $I=\left\{\left(\dfrac{n}{p}\right)^i \cdot p^j \mid i,j\geqslant 0\right\}$中每个数关于集合 $P=\left\{\prod_{a=0}^{l}(x+a)^{e_a} \mid e_a\geqslant 0\right\}$中每个多项式都具有性质(I)。

基于这些集合定义两个群，它将对证明起到关键的作用。

第一个群是所有属于 I 的数 mod r 的剩余的集合，它是 Z_r^* 的子群，因$(n,r)=(-p,r)=1$，令这个群为 G_1，$|G_1|=t$。

因 G_1 是由 n 和 p mod r 生成的，指数 $O_r(n)>\log^2 n$，$t>\log^2 n$。

第二个群 G_2，它需要关于有限域 F_p 的分圆多项式的若干事实。令 $Q_r(x)$是第 r 个关于 F_p 的分圆多项式，$Q_r(x)\mid x^r-1$。将它分解成不可化约的因子，次方为 $O_r(p)$，令 $h(x)$是这样的一个不可化约的因子，因 $O_r(p)>1$，$h(x)$的次方大于 1，G_2 是由在 $F=\dfrac{F_p(x)}{h(x)}$ 域由 $x+1, x+2, \cdots, x+l$ 生成的群，是 F 乘法群的子群。

引理 3 (H. Lenstra Jr)$|G_2|\geqslant\dbinom{t+l}{t-1}$。

证 首先注意，因 $h(X)$是分圆多项式 $Q_r(X)$的因子，X 是在 F 的单位元素的第 r 个原根。

现在证明两个在 P 集合的次方小于 t 的不同多项式将映射到 G_2 的不同元素。假定 $f(X)$ 和 $g(X)$是属于 P 的两个多项式。假定在 F，$f(X)=g(X)$，令 $m\in I$。我们也一定有在 $F[f(X)]^m=[g(X)]^m$，因 m 是关于 f 和 g 具有性质(I)。$h(X)\mid X^r-1$，故在 $F[f(X^m)]=g(X^m)$，这说明 X^m 是多项式 $Q(Y)=f(Y)-g(Y)$的根，$m\in G_1$，因$(m,r)=1$，G_1是 Z_r^* 的子群，每一个这样的 X^m 是单位圆的第 r 个原根，将有$|G_1|=t$ 个 $Q(Y)$在 F 的根，无论如何 $Q(Y)$的次方小于 t，由于 f 和 g 的选择，这导致矛盾，所以在 F $f(X)\neq g(X)$。

注意在 F_p，$1\leqslant i\neq j\leqslant l$，$l=\lfloor\sqrt{\Phi(r)}\log n\rfloor<\sqrt{r}\log n<r$，且 $p>r$，所以元素 $X, X+1, \cdots,$

$X+l$ 在 F 全不相同，同样地，$h(X)$ 的次方大于 1，在 F $X+a\neq 0$，对每个 a，$0\leqslant a\leqslant l$，所以至少有 $l+1$ 个在 G_2 不同的次方 1 的多项式，故至少有 $\binom{t+l}{t-1}$ 个在 G_2 的不同多项式，次方 $<t$。证毕。

引理 4　若 n 不是 p 的幂，则 $|G_2|\leqslant n^{\sqrt{t}}$。

证　考虑 I 的下列子集

$$\hat{I}=\left\{\left(\frac{n}{p}\right)^i p^j \mid 0\leqslant i,j\leqslant\lfloor\sqrt{t}\rfloor\right\}$$

如果 n 不是 p 的幂，则 $\hat{I}$ 有 $(\lfloor\sqrt{t}+1\rfloor)^2>t$ 不同的数，因 $|G_1|=t$ 至少有两个数在 $\hat{I}$ mod r 相等，设为 m_1 和 m_2，$m_1>m_2$；故

$$X^{m_1}\equiv X^{m_2}(\bmod\ (X^r-1))$$

令 $f(X)\in P$，则

$$\begin{aligned}[f(X)]^{m_1}&\equiv f(X^{m_1})\ (\bmod\ (X^r-1,p))\equiv f(X^{m_2})\ (\bmod\ (X^r-1,p))\\&\equiv[f(X)]^{m_2}(\bmod\ (X^r-1,p))\end{aligned}$$

所以在 F 上：

$$[f(X)]^{m_1}\equiv[f(X)]^{m_2}(\bmod\ (X^r-1))$$

故 $f(X)\in G_2$ 是多项式 $Q'(Y)=Y^{m_1}-Y^{m_2}$ 的在 F 的根（这个公式是 A. Kalai、A. Sahai、M. Sudan[KSS]提供的结果）。$f(X)$ 是 G_2 的任意元素，多项式 $Q'(Y)$ 最少有 $|G_2|$ 个在 F 的不同的根，$Q'(Y)$ 的次方是 $m_1\leqslant\left(\frac{n}{p}\cdot p\right)^{\lfloor\sqrt{t}\rfloor}\leqslant n^{\sqrt{t}}$，此证 $|G_2|\leqslant n^{\sqrt{t}}$ 证毕。

引理 5　若算法输出“素数”，则 n 是素数。

证　假定算法输出“素数”，由引理 5，说明 $t=|G_1|$，$l=\lfloor\sqrt{\Phi(r)}\log n\rfloor$，

$$\begin{aligned}|G_2|&\geqslant\binom{t+l}{t-1}\geqslant\binom{l+1+\lfloor\sqrt{t}\log n\rfloor}{\lfloor\sqrt{t}\log n\rfloor}\quad(\text{因 } t>\sqrt{t}\log n)\\&\geqslant\binom{2\lfloor\sqrt{t}\log n\rfloor+1}{\lfloor\sqrt{t}\log n\rfloor}\quad(\text{因 } l=\lfloor\sqrt{\Phi(r)}\log n\rfloor\geqslant\lfloor\sqrt{t}\log n\rfloor)\\&>2^{\lfloor\sqrt{t}\log n\rfloor+1}\quad(\text{因}\lfloor\sqrt{t}\log n\rfloor>\lfloor\log^2 n\rfloor\geqslant 1)\\&\geqslant n^{\sqrt{t}}\end{aligned}$$

由引理 5，$|G_2|\leqslant n^{\sqrt{t}}$，若 n 不是 p 的幂，所以 $n=p^k$，$k>0$，若 $k>1$，则算法在 S1 输出“合数”，所以 $n=p$。

定理证完。

定理 5-3：m 是关于 $f(x)$ 和 $g(x)$ 具有性质(I)，则 m 是关于 $f(x)g(x)$ 具有性质(I)。

证　$[f(x)\cdot g(x)]^m\equiv[f(x)]^m\cdot[g(x)]^m\equiv f(x^m)\cdot g(x^m)(\bmod\ (X^r-1,p))$ 证毕

5.10　复杂性分析

定理 5-4：算法的时间复杂性近似于 $O(\log^{\frac{21}{2}n})$。

证　S1 算法的时间近似于 $O(\log^3 n)$。

S2 求 r 使 $O_r(n)>\log^2 n$，可以通过 r 的搜索，若 $n^k\not\equiv 1(\bmod r)$，$k\leqslant\log^2 n$，最多 $O(\log^2 n)$ 次$(\bmod r)$ 的乘法，需时 $O(\log^2 n\log r)$，由引理 2，只有 $O(\log^2 n)$个不同的 r 需要测试，故全体的时间复杂性为 $O(\log^7 n)$。

S3 计算 r 次的 gcd，每次时间为 $O(\log n)$，故全部时间复杂性为 $O(r\log n)=O(\log^6 n)$。

S4 的时间复杂性正好是 $O(\log n)$。

S5 要证明$\lfloor\sqrt{\Phi(r)}\log n\rfloor$个方程，每个需 $O(\log n)$ 次 r 次方多项式的乘法，多项式的系数规模为 $O(\log n)$，S5 的时间复杂性为 $O(r\sqrt{\Phi(r)}\cdot\log^3 n)=O(r^{\frac{3}{2}}\log^3 n)=O(\log^{\frac{21}{2}}n)$，与其他相比它是最高级的，所以算法的复杂性也就是 $O(\log^{\frac{21}{2}}n)$。

5.11　改进意见

2004 年的 AKS 算法实际上是不现实的，时间复杂性的改进可通过对 r 的计算的改进(引理 2 所作)，最好的可能将是 $r=O(\log^2 n)$，这样算法复杂性将是 $O(\log^6 n)$，事实上有两个猜想支持了这个可能性。

Artin 猜想：已知任意 $n\in\mathbf{N}$，它不是完全平方，素数 $q\leqslant m$ 的数目，使 $O_q(n)=q-1$，近似于 $A(n)\cdot\dfrac{m}{\ln m}$，$A(n)$是 Artin 常数，$A(n)>0$。

Sophie-Germain 素数密度猜想：素数 $q\leqslant m$，使 $2q+1$ 也是素数，数目接近于$\dfrac{2c_2 m}{\ln^2 m}$，其中 c_2是常数(大约为 0.66)，这样的素数称为 Sophie-Germain 素数。

Artin 猜想若成立，$m=O(\log^2 n)$，则有一$r=O(\log^2 n)$ 有所求的性质，有若干进展关于 Artin 猜想。

第二个猜想若成立，可得 $r=O(\log^2 n)$，使算法复杂性降为 $O(\log^6 n)$。

5.12　2002 年的 AKS 算法

S1 若 $n=a^b$，则输出“合数”。

S2 求素数 r 使 $\gcd(r,n)=1$，$r-1$ 的最大素因子 $q\geqslant 4\sqrt{r}\log n$，$n^{\frac{n-1}{q}}\not\equiv 1(\bmod r)$。

S3 $\forall a\in(1,2,\cdots,\lfloor 2\sqrt{r}\log n\rfloor)$，若 $(X-a)^n\not\equiv X^n-a(\bmod (X^r-1,n))$，则输出“合数”。

S4 输出“素数”。

算法复杂性：$O(\log^{12} n)$。

习　　题

1. 求 Jacobi 符号$\left(\frac{a}{n}\right)$的编程。
2. 完成 Miller-Rabin 测试法的编程。

附录 A

Chebyshev 引理 $\prod_{p<2m} p \geqslant 2^m, m < 32$。

证　$m<32$ 不等式成立

$$\binom{2m}{m}=\frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2m-1)}{2 \cdot 4 \cdot \cdots \cdot (2m)} \cdot 2^{2m}$$

$$=\frac{1}{\sqrt{2}} \cdot \frac{3}{\sqrt{2} \cdot \sqrt{4}} \cdot \frac{5}{\sqrt{4} \cdot \sqrt{6}} \cdots \frac{2m-1}{\sqrt{2m-2} \cdot \sqrt{2m}} \cdot \frac{1}{\sqrt{2m}} 2^{2m}$$

$$>\frac{2^{2m}}{\sqrt{4m}} = 2^{2m-\frac{1}{2}\log(4m)}$$

素数 p 的次方除 m！是

$$\left\lfloor\frac{m}{p}\right\rfloor+\left\lfloor\frac{m}{p^2}\right\rfloor+\cdots+\left\lfloor\frac{m}{p^{\lfloor\log_p m\rfloor}}\right\rfloor$$

所以

$$\log\binom{2m}{m}=\sum_{p\leqslant 2m}\log p\sum_{k=1}^{\log_p 2m}\left(\left\lfloor\frac{2m}{p^k}\right\rfloor-2\left\lfloor\frac{m}{p^k}\right\rfloor\right)$$

$$\leqslant\sum_{p\leqslant 2m}\lg p+\sum_{p\leqslant\sqrt{2m}}\lg p\sum_{k=2}^{\log_p 2m}\left(\left\lfloor\frac{2m}{p^k}\right\rfloor-2\left\lfloor\frac{m}{p^k}\right\rfloor\right)$$

$$\leqslant\sum_{p\leqslant 2m}\lg p+\sum_{p\leqslant\sqrt{2m}}\lg p\left(\frac{\lg 2m}{\lg p}-1\right)\leqslant\sum_{p\leqslant 2m}\lg p+\sum_{p\leqslant\sqrt{2m}}(\lg 2m-1)$$

$$\leqslant\sum_{p\leqslant 2m}\lg p+\frac{1}{2}\sqrt{2m}(\lg 2m-1)\quad(\sqrt{2m}\geqslant 8,\text{即 } m\geqslant 32)$$

$$\sqrt{2m}>\lg 4m>\lg 2,\quad m\geqslant 32$$

$$\prod_{p\leqslant 2m}p\geqslant 2^{2m-\frac{1}{2}\lg 4m-\frac{1}{2}\sqrt{2m}(\lg 2m-1)}\geqslant 2^{2m-\frac{1}{2}\sqrt{2m}\lg 2m}\geqslant 2^{2m}$$

第 6 章　零知识证明简介

6.1　概　　念

设证明者 P 掌握某些秘密信息，也可以是已获得长期没有解决问题的解法，信息本身是可以验证的，即可以通过具体的步骤来验证其正确性。V 是验证者，P 设法使 V 相信他确实掌握这些信息，当然 P 可以直截了当告诉 V 他掌握的信息，这样不是零知识证明。P 想说服 V 他确实无误掌握这些信息，但要求连 1 比特的秘密也不泄露，从而 V 无法获得秘密的本身。最简单的步骤，以 $n=pq$ 为例，n 公开，若 A 已掌握 p 和 q，P 要求 V 相信如此信息：

S1 V 随机选择一大数 x，计算 $x^2 \pmod n$ 并将结果告诉 P。

S2 P 解出 x，并将 x 告诉 V。

V 知道求解 $x^2 \pmod n$ 并等价于 n 的因数分解，并不掌握 p 和 q，求平方根是一难题。P 将 x 告诉 V，V 毫无所得，因为他早已掌握 x 的值。多次重复以上步骤，一直到 V 成功地掌握 p 和 q 的可能性是渺茫的。

例 6-1　交互过程的零知识证明。

身份证明的协议：每一用户，设 A，秘密选一正整数 α_A，并计算 $y_A=g^{\alpha_A}$，并用 (A, y_A) 形式分布在通讯录上，每一用户都有一通讯录，A 向 B 证明自己的身份，步骤如下：

(1) A 向 B 送去一整数 α。

(2) B 收到后随地选择一正整数 R，计算 $y_2=g^R$ 送给 A。

(3) A 计算 $(y_A)^R=g^{\alpha_A R}$，A 将 $y_3=g^{\alpha_A R}$ 送给 B。

(4) B 计算 $(y_A)^R=g^{\alpha_A R}$，并检查 $(y_A)^R=y_3$?，等号若成立，A 的身份便得到证明。

但协议不是零知识的，因为若 B 送去 $y_2=R$，他将获得 $y_3=\alpha^R$，这结果并非他所能得到的。

例 6-2　若已知正整数 x 和 y，$0<y<x$，$\gcd(x, y)=1$，P 宣称他知道不存在 $E\in \mathbf{Z}$，使 $z^2\equiv y \pmod x$。

验证者 V 便产生一组序列 $z_1, z_2, \cdots, z_n$ 及 0，1 序列 $b_1, b_2, \cdots, b_n$ 满足 $0<z_i<x$，$(z_i, x)=1$，$i=1,2,\cdots,n$，计算：

$$w_i\equiv\begin{cases} z_i^2 \pmod x, & b_i=0, \\ z_i^2 y \pmod x, & b_i=1, \quad i=1,2,\cdots,n \end{cases}$$

P 对此进行判断：

$$c_i\equiv\begin{cases} 0, & \text{存在 } z_i\equiv w_i \pmod x \\ 1, & \text{其他} \end{cases}$$

P 将 $c_1, c_2, \cdots, c_n$ 送 V。

若对所有的 i，$c_i = b_i$，则 P 断定不存在 z 使 $z^2 \equiv y \pmod{x}$ 得到证明，表面 V 得到的都是他自己知道的事，但事实上 P 已向 V 泄露了 V 本来不掌握的信息：即不存在 z 满足 $z^2 \equiv y \pmod{x}$。

6.2　身份的零知识证明

智能卡、信用卡等身份鉴别技术可能由于敌方和不诚实的验证方合作可能获得卡的拷贝，或知道 $I(P)$ 身份从事假冒 P 从事非法活动。解决办法是利用零知识证明技术，P 可以不透露 $I(P)$ 的一个比特使 V 确实 P 掌握 $I(P)$。

(1) 假定存在一可信赖的机构，它的职责在于公布模数 n，$n = pq$；p、q 为大素数，p 和 q 都是 mod 4 与 3 同余。

$I(P)$ 必须包含 P 的许多信息，规定必须包含保密身份的 k 个数：$c_1, c_2, \cdots, c_k$，$1 \leqslant c_i < p$，$i = 1, 2, \cdots, k$，还有他的公开身份另外 k 个数：$d_1, d_2, \cdots, d_k$，$1 \leqslant d_i < p$，$i = 1, 2, \cdots, k$，而且 $d_j c_j^2 \equiv \pm 1 \pmod{n}$，$i = 1, 2, \cdots, k$。

验证者 V 知道 P 的公开身份，P 为了使 V 相信他掌握 $I(P)$，下面 4 个步骤算是一轮，轮数越多 P 作假的概率越小。

S1 P 选一随机 r，计算 $\pm r^2 \pmod{n}$，P 取其一送 V。

S2 V 从 $\{1, 2, \cdots, k\}$ 中选一子集告诉 P。

S3 P 告诉 V：

$$y \equiv r T_c \pmod{n}$$

其中 $T_c \equiv \prod_{j \in S} c_j$。

S4 V 验证：

$$x = \pm y^2 T_d \pmod{n}?$$

其中 $T_d \equiv \prod_{j \in S} d_j$，若等号成立，一轮检验通过，否则予以拒绝。

因 $d_j c_j^2 \equiv \pm 1 \pmod{n}$，$j = 1, 2, \cdots, k$，所以 $y^2 T_d \equiv r^2 T_c^2 T_d \equiv r^2 \prod_{j \in S} c_j^2 d_j \equiv \pm r^2 \equiv \pm x \pmod{n}$。

随机数 r 是必要的，否则 V 选 $S \in \{j\}$，从而找到 c_j，对 c_j 要求 $(c_j, n) = 1$，$j = 1, 2, \cdots, k$，否则 n 可能被因数分解。

例 6-3　可信赖机构宣布 $n = 2773$。

P 的秘密 $I(P)$ 包含：

$$c_1 = 1901, c_2 = 2114, c_3 = 1509, c_4 = 1400, c_5 = 2001, c_6 = 119,$$
$$c_4^2 \pmod{n} \equiv 2262, c_5^2 \pmod{n} \equiv 2562, c_6^2 \equiv 296$$

P 选择公开身份，有

$$d_1 = 53, d_2 = 2678, d_3 = 1207, d_4 = 1183, d_5 = 2681, d_6 = 2595$$

它们满足 $d_j c_j^2 \equiv \pm 1 \pmod{n}$。

假定 P 选 $r = 1221$，计算

$$-r^2 \equiv -1\,490\,811 \equiv 1033 \pmod{n}$$

$x = 1033$，P 将 x 告诉 V，V 选子集 $S = \{1, 4, 5, 6\}$ 告诉 P，P 计算：

$T_c = 1901 \times 1400 \times 2001 \times 119 \equiv 96 \pmod n$

$y \equiv rT_c \pmod n \equiv 1221 \times 96 \equiv 117216 \pmod n \equiv 750$

V 收到 y 计算：

$T_d = 81 \times 1183 \times 2681 \times 2595 \pmod n \equiv 1116$

$y^2 T_d = (750)^2 \times 1116 = 627\,750\,000 \equiv 1033 \pmod n$

验证通过。

6.3 Fiat-Shamir 协议适于网上身份验证

假定 P 的身份有 k 个秘密的数：$x_{p_1}, x_{p_2}, \cdots, x_{p_k}$，令 $n = pq$，作 $y_{p_i} \equiv x_{p_i}^2 \pmod n$，公开文件上在 P 的姓名后面记录上 ID：$y_{p_1}, y_{p_2}, \cdots, y_{p_k}$。

S1 P 随机选一数 $r \in Z_n$ 计算 $r^2 \pmod n$。P 给 V 送去(P, r^2)。

S2 V 给 P 送去 $b = (b_1, b_2, \cdots, b_k)$，$b_i$ 是随机产生的 0 或 1，$b_i \in \{0,1\}$，$i = 1,2,\cdots,k$。

S3 P 计算 $b = rc_1c_2\cdots c_k$，并将 y 送 V，其中 $c_i = \begin{cases} 1, & b_i = 0 \\ 0, & b_i = 1 \end{cases}$，$i = 1,2,\cdots,k$，

S4 V 检验，若 $y^2 = r^2 \prod_{i=1}^{k} (y_{p_i}^{b_i}) \pmod n$，则接受，否则拒绝。实际上因不掌握 y_{p_i}，$i = 1,2,\cdots,k$，而欺骗成功的概率是$\frac{1}{2^k}$。

6.4 Schnorr 身份验证

(1) Schnorr 的身份验证是基于求离散对数的困难性系数参数是 p, q 两个素数，q 是 $p-1$ 的素数因数，$g \not\equiv 1 \pmod q$，P 取 x_p，计算 $y_p \equiv g^{x_p} \pmod p$。

P 已知：x_p, y_p, p, q, g，V 已知 p, q, g。

S1 (1)P 产生一随机数 $r_1 \in GF(p)$，$r_1 \neq 0$，

(2) 计算 $S = g^r \pmod p$，

(3) P 将(y_p, S)送 V。

S2 V 产生一随机数 r_2，并将 r_2 寄给 P。

S3 P 计算 $v \equiv r_1 + r_2 x_p \pmod p$，并将 v 送 V。

S4 V 校验 $g^v = S\,(y_p)^{r_2}$？

若相等则接受，否则予以拒绝。

因 $g^v \equiv g^{(r_1 + r_2 x_p)} \pmod p \equiv g^{r_1} (g^{x_p})^{r_2} \pmod p \equiv g^{r_1} \cdot (y_p)^{r_2} \pmod p \equiv S \cdot (y_p)^{r_2}$。

6.5 Feige-Fiat-Shamir 身份验证协议

定义 $a \in Z_n^*$，a 称为 mod n 的平方剩余，若存在 $x \in Z_n^*$ 使 $x^2 \equiv a \pmod n$，若不存在这样的 x，则称 a 为非平方剩余，mod n 的所有平方剩余的集合表以 Q_n，所有的非平方剩

余，则表以 $\bar{Q}_n$。

由定义 $0 \notin Z_n^*$，故 $0 \notin Q_n$，$0 \notin \bar{Q}_n$。

例如，$\alpha=6$，是 Z_B^* 的生成元素，α 的幂列表如表 6-1 所示。

表 6-1　α^i(mod 13)的值

i	0	1	2	3	4	5	6	7	8	9	10	11	12
α^i(mod 13)	1	6	10	8	9	2	12	7	3	5	4	11	1

$$Q_{13}=\{1,3,4,9,10,12\},\bar{Q}_{13}=\{2,5,6,7,8,11\},$$

$n=pq$，p 和 q 都是奇素数，$a \in Z_n^*$ 是 mod n 的平方剩余，当且仅当 $a \in Q_p$ 和 $a \in Q_q$，故 $|Q_n|=|Q_p||Q_q|=\frac{1}{4}(p-1)(q-1)$，$|\bar{Q}_n|=\frac{3(p-1)(q-1)}{4}$。

定义 6-1　合数 $n=pq$，p 和 q 是不同素数，但 mod 4 都和 3 同余，$n=pq$ 是一 Blum 数，$n=pq$ 是一 Blum 数，$a \in Q_n$，则 mod n，a 有 4 个平方根，每一个根都在 Q_n。

6.6　Feige-Fiat-Shamir 身份验证

Jacobi 符号的计算。

输入 $n>3$ 的奇整数，整数 a，$0 \leqslant a<n$。

输出 $\left(\frac{a}{n}\right)$，(n 是素数时为勒让德符号)。

S1 若 $a=0$，则输出(0)。

S1 若 $a=1$，则输出(1)。

S3 将 a 写成 $2^l a_1$，a_1 是奇整数。

若 e 是偶数则 $S \leftarrow 1$，否则 $S \leftarrow 1$ 若 $n \equiv 1 (\bmod 8)$ 或 $m \equiv 7 (\bmod 8)$。

或 $S \leftarrow -1$ 若 $n \equiv 3 (\bmod 8)$ 或 $n \equiv 5 (\bmod 8)$。

S4 若 $n \equiv 3 (\bmod 4)$，$a_1 \equiv 3 (\bmod 4)$ 则 $S \leftarrow -S$。

S5 $n_1 \leftarrow n (\bmod a_1)$。

S6 若 $a_1=1$ 则输出(S)，否则输出$\left(\left(\frac{a_1}{n_1}\right)\right)$。

Feige-Fiat-Shamir 身份验证如下：

(1) 系统的参数，可信赖的中心 T 公布 $n=pq$，p 和 q 都(mod 4)和 3 同余，使其难于因数分解，(n 是 Blum 数，和 -1 是 mod n 的平方剩余，和雅科比符号取 $+1$)整数 k 和 t 为秘密参数。

(2) 选每个单元保密，每个元素 A 做：

a. 选 k 个随机整数 $S_1,S_2,\cdots,S_k$，$1 \leqslant S_i \leqslant n-1$，$k$ 个随机比特 $b_1,b_2,\cdots,b_k$，$\gcd(S_i,n)=1$，保证 n 不被因数分解。

b. 计算 $v_i \equiv (-1)^{b_i}(S_i^2)^{-1} (\bmod n)$，$1 \leqslant i \leqslant k$。

(这允许 v_i 全体和 n 互素，雅科比符号 $+1$，一个技术条件证明选 n 没有保密信息泄

露，显然选 v_i 有平方根）。

c. A 证明自己用非保密方法（如照片）给 T，后来给 A 公钥$(S_1, S_2, \cdots, S_k) \bmod n$，T 确认每个 v_i 有关于 n 的雅科比符号为+1。

（3）信息协议：

t 轮每一次：

$A \to B$：$x = r^2 \bmod n$。

$A \leftarrow B$：$(e_1, e_2, \cdots, e_k)$，$e_i \in \{0,1\}$。

$A \to B$：$y = r\prod_{e_j=1} S_j(\bmod n)$。

（4）协议行动，下面步骤执行 t 次，B 接受 A 的身份，若所有 t 轮都成功。假定 B 有 A 的可信的公钥$(v_1, \cdots, v_k; n)$，否则一个证明可送到信息（1）。

a. A 随机选整数 r，$1 \leqslant r \leqslant n-1$ 和随机比特 b，计算：

$x \equiv (-1)^b \cdot r^2 (\bmod n)$，并送 x 到 B。

b. B 送 A 随机的 k 比特向量$(e_1, e_2, \cdots, e_k)$。

c. A 计算 $y \equiv r\prod_{j=1}^{k} S_j^{e_j} (\bmod n)$。

d. B 计算 $Z \equiv y^2 \cdot \prod_{j=1}^{k} v_j^{e_j} (\bmod n)$，证明 $z = \pm x$，和 $z \neq 0$。

（最后防对方成功选 $r=0$）

例 6-4 权威中心 T 选 $p=683$，$q=811$，$n=pq=553\,913$，$k=3$，$t=1$。

1. A 做。

a. 选 3 个随机整数 $S_1=157$，$S_2=43\,215$，$S_3=4646$。

3 个比特：$b_1=1$，$b_2=0$，$b_3=1$。

b. 计算 $v_1=441\,845$，$v_2=338\,402$，$v_3=124\,423$。

c. A 的公钥是（441 845，338 402，124 423，553 913），密钥是（157，43 215，4646）。

2. 信息的总体交换。

3. （1）A 选 $r=1279$，$b=1$，计算 $x=25\,898$ 送 B。

（2）B 送 A 3 个比特向量（0，0，1）。

（3）A 计算 $y=r \cdot S_3 (\bmod n)=403\,104$，并送 B。

（4）B 计算 $z \equiv y^2 \cdot v_3 (\bmod n) \equiv 25\,898$，接收 A 的身份，因 $z=+x$，$z \neq 0$。

习　　题

试举例说明 Fiat-Shamir；Schnhorr；Feige-Fiat-Shamir 3 个身份验证。

第 7 章　大数快速算法与求离散对数

7.1　数的 *m* 进制表示

(1) 整数 n 的 m 进制表示：$n=(a_k a_{k-1}\cdots a_0)_m=a_k m^k+a_{k-1}m^{k-1}+\cdots+a_1 m+a_0$。

令 $n_0=n, n_1=\left\lfloor\frac{n_0}{m}\right\rfloor=a_k m^{k-1}+a_{k-1}m^{k-2}+\cdots+a_1$,余数 $r_1=a_0$

$n_2=\left\lfloor\frac{n_1}{m}\right\rfloor=a_k m^{k-2}+a_{k-1}m^{k-3}+\cdots+a_2$,余数 $r_2=a_1$

…

$n_{i+1}=\left\lfloor\frac{n_i}{m}\right\rfloor=a_k m^{k-i-1}+a_{k-1}m^{k-i-2}+\cdots+a_{i+1}$,余数 $r_{i+1}=n_i$

$i=1,2,\cdots,k$

一直到 $n_k<m$ 为止。

例 7-1　$n=15, m=2$,即求 15 的二进制表示。

$$\left\lfloor\frac{15}{2}\right\rfloor=7, r_1=a_0=1$$

$$\left\lfloor\frac{7}{2}\right\rfloor=3, r_2=a_1=1$$

$$\left\lfloor\frac{3}{2}\right\rfloor=1, r_3=a_2=1$$

$$\left\lfloor\frac{1}{2}\right\rfloor=0, r_4=a_3=1,\text{故 } 15=(1111)_2$$

(2) 计算机常用 2^4 进制表示,即十六进制表示。

以 $n=1323$ 为例：

$$\left\lfloor\frac{1323}{2}\right\rfloor=661, a_0=1, \left\lfloor\frac{661}{2}\right\rfloor=330, a_1=1$$

$$\left\lfloor\frac{330}{2}\right\rfloor=165, a_2=0, \left\lfloor\frac{165}{2}\right\rfloor=82, a_3=1$$

$$\left\lfloor\frac{82}{2}\right\rfloor=41, a_4=0, \left\lfloor\frac{41}{2}\right\rfloor=20, a_5=1$$

$$\left\lfloor\frac{20}{2}\right\rfloor=10, a_6=0, \left\lfloor\frac{10}{2}\right\rfloor=5, a_7=0$$

$$\left\lfloor\frac{5}{2}\right\rfloor=2, a_8=1, \left\lfloor\frac{2}{2}\right\rfloor=0, a_9=0$$

$\left\lfloor \frac{1}{2} \right\rfloor = 0, a_{10} = 1,$

$1323 = (10\ 100\ 101\ 011)_2 = ((101)_2(0010)_2(1011)_2)_{16}$

$(101)_2 = 5, (0010)_2 = 2, (1011)_2 = 11$

在十六进制中，用 A 表示 10，B 表示 11，C 表示 12，D 表示 13，E 表示 14，F 表示 15；故 $1323 = (52B)_{16} = O_x 52B$。

7.2 多位数的运算

（1）两个 b 进制 $n+1$ 位的正整数 x 和 y 的加法运算：

令 $x = (x_n x_{n-1} \cdots x_1 x_0)_b, y = (y_n y_{n-1} \cdots y_1 y_0)_b$，求 $x+y$。

S1 $C \leftarrow 0, i \leftarrow 0$，

S2 若 $i \leqslant n$ 作

始 $w_i \leftarrow x_i + y_i + C \pmod b$

若 $w_i < b$，则 $C \leftarrow 0$，否则 $C \leftarrow 1, i \leftarrow i+1$，转 S2 **终**，否则作 $w_{n+1} \leftarrow C$。

S3 输出 $(w_{n+1} w_n \cdots w_1 w_0)_b$。

（2）多位数的减法：

已知两个 $n+1$ 位 b 进制数 x, y，且 $x > y$，求 $x - y = (w_n w_{n-1} \cdots w_1 w_0)_b$。

S1 $C \leftarrow 0, i \leftarrow 0$，

S2 若 $i \leqslant n$ 则作

始 $w_i \leftarrow (x_i - y_i + C) \pmod b$，

若 $w_i > 0$，则做 $C \leftarrow 0$，否则 $C \leftarrow -1, i \leftarrow i+1$，转 S2 **终**。

S3 输出 $(w_n w_{n-1} \cdots w_1 w_0)_b$。

（3）多位数的乘法：

设 $x = x_n b^n + x_{n-1} b^{n-1} + \cdots + x_1 b + x_0$

$y = y_t b^t + y_{t-1} b^{t-1} + \cdots + y_1 b + y_0$

$$x \cdot y = (x_n b^n + x_{n-1} b^{n-1} + \cdots + x_1 b + x_0) \cdot (y_t b^t + y_{t-1} b^{t-1} + \cdots + y_1 b + y_0)$$
$$= w_{n+t+1} b^{n+t+1} + w_{n+t} b^{n+t} + \cdots + w_1 b + w_0$$

S1 $w_i \leftarrow 0, i = 1, 2, \cdots, n+t+1, i \leftarrow 0$。

S2 若 $i \leqslant t$ 则作

始 $C \leftarrow 0, j \leftarrow 0$，转 S1 终，否则转 S5。

S3 若 $j \leqslant n$，则作

始 $(uv)_b = w_{i+j} + (x_j y_i) + C$，

$w_{ij} \leftarrow v, C \leftarrow u, j \leftarrow j+1$，转 S3 **终**，否则转 S4。

S4 $w_{i+n+1} \leftarrow u, i \leftarrow i+1$，转 S2。

S5 输出 $((w_{n+t+1} \cdots w_1 w_0)_b)$。

例 7-2 $x = x_3 x_2 x_1 x_0 = 9274, y = y_2 y_1 y_0 = 847, n = 3, t = 2$，见表 7-1。

表 7-1　例 7-2 表

i,j	C	$w_{ij}+x_j y_i+C$	u	v	w_6	w_5	w_4	w_3	w_2	w_1	w_0
0 1	0	0+28+0	2	8	0	0	0	0	0	0	8
1	2	0+49+2	5	1	0	0	0	0	0	1	8
2	5	0+14+5	1	9	0	0	0	0	9	1	8
3	1	0+63+1	6	4	0	0	4	4	9	1	8
1 1	0	1+16+0	1	17	0	0	6	4	9	7	8
1	1	9+28+1	3	8	0	0	6	4	8	7	8
2	3	4+8+3	1	5	0	0	6	5	8	7	8
3	1	6+36+1	4	3	0	4	3	5	8	7	8
2 1	0	8+32+0	4	0	0	4	3	5	0	7	8
1	4	5+56+4	6	5	0	4	3	5	0	7	8
2	6	3+16+6	2	5	0	4	5	5	0	7	8
3	2	4+72+2	7	8	7	8	5	5	0	7	8

```
      9274
×      847
----------
     64918
    37096
+) 74192
----------
   7855078
```

```
     64918
+)  390960
----------
    455878
```

（4）平方：

输入正整数 $x=(x_t x_{t-1}\cdots x_1 x_0)_b$。

输出：x^2 的 b 进制表示。

S1 $w_i \leftarrow 0, i=0,1,2,\cdots,2t+1, i\leftarrow 0$。

S2 若 $i\leqslant t-1$ 则作

始　$(uv)_b \leftarrow w_{2i}+x_i \cdot x_i, w_{2i}\leftarrow v, v\leftarrow u, j\leftarrow i+1$，

A 若 $j\leqslant t-1$ 则作

始　$(uv)_b \leftarrow w_{i+j}+2x_j \cdot x_i+C, w_{i+j}\leftarrow v, C\leftarrow u$，

$j\leftarrow i+1$，转 A **终**，

$w_{i+t}\leftarrow u, i\leftarrow u+1$，转 S2。

终。

S3 输出$((w_{2t-1}w_{2t-2}\cdots w_1 w_0)_b)$。

例 7-3　求$(989)^2, t=3, b=10$，见表 7-2。

表 7-2　例 7-3 表

i,j	$w_{2i}+x_i^2$	$w_{i+j}+2x_jx_i+C$	u	v	w_5	w_4	w_3	w_2	w_1	w_0
0 —	0+81	—	8	1	0	0	0	0	0	1
1	—	0+2·8·9+8	15	2	0	0	0	0	2	1
2	—	0+2·9·9+15	17	7	0	0	0	7	2	1
			17	7	0	0	17	7	2	1
1 —	7+64		7	1	0	0	17	1	2	1
2		17+2·9·8+7	16	8	0	0	8	1	2	1
			10	8	0	16	8	1	2	1
2 —	16+81	—	9	7	0	7	8	1	2	1
			9	7	9	7	8	1	2	1

```
       989
×      989
──────────
      8901
     7912
+）  8901
──────────
    978121
```

（5）除法：

输入正整数 $x=(x_nx_{n-1}\cdots x_1x_0)_b$，$y=(y_ty_{t-1}\cdots y_1y_0)_b$，$n\geqslant t\geqslant 1$，$y_t\neq 0$。

输出 $q=(q_{n-t}\cdots q_1q_0)_b$，$r=(r_t\cdots r_1r_0)_b$，使 $x=qy+r$，$0\leqslant r<y$。

S1 $q_j\leftarrow 0$，$j=0,1,\cdots,(n-t)$。

S2 若 $x\geqslant yb^{n-t}$，则

始 $q_{n-t}\leftarrow q_{n-t}+1$，$x\leftarrow x-yb^{n-t}$，转 S2 **终**，否则作 $i\leftarrow n$。

S3 若 $i\geqslant t-1$ 则

始　若 $x_i=y_i$，则 $q_{i-t-1}\leftarrow b-1$ 否则 $q_{i-t-1}\leftarrow\left\lfloor\dfrac{(x_ib+x_{i-1})}{y_t}\right\rfloor$，

　A 若$(q_{i-t-1}(y_tb+y_{t-1})>x_ib^2+x_{i-1}b+x_{i-2})$则作

　始　$q_{i-t-1}\leftarrow q_{i-t-1}-1$，转 A **终**，

$$x\leftarrow x-q_{i-t-1}yb^{i-t-1},$$

若$x<0$ 则作

始　$x\leftarrow x+yb^{i-t-1}$，$q_{i-t-1}\leftarrow q_{i-t-1}-1$，**终**。

$i\leftarrow i-1$，转 S3。

S4 $r\leftarrow x$。

S5 输出$((q,r))$。

例 7-4　$x=721\ 948\ 327$，$y=84\ 461$，$n=8$，$t=4$，见表 7-3。

表 7-3　例 7-4 表

i	q_4	q_3	q_2	q_1	q_0	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
—	0	0	0	0	0	7	2	1	9	4	8	3	2	7
8	0	0	0	0	0	7	2	1	9	4	8	3	2	7
		8	0	0	0		4	6	2	6	0	3	2	7
7		8	5	0	0			4	0	2	9	8	2	7
6		8	5	5	0			4	0	2	9	8	2	7
		8	5	4	0				6	5	1	3	8	7
5		8	5	4	8				6	5	1	3	8	7
		8	5	4	7					6	0	1	6	0

$q=8547, r=60160$。

(6) 大数模幂运算：

当 m, r, n 都是很大的整数时如何求 $m^r \pmod n$ 的问题。

若将 r 化为二进制数：

$$R_0 = r = a_k 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2 + a_0, a_i \in (0,1), 0 \leqslant i \leqslant k$$

$$R_1 = \left\lfloor \frac{R_0}{2} \right\rfloor = a_k 2^{k-1} + a_{k-1}2^{k-2} + \cdots + a_1, r_1 = a_0$$

$$R_2 = \left\lfloor \frac{R_1}{2} \right\rfloor = a_k 2^{k-2} + a_{k-1}2^{k-3} + \cdots + a_2, r_2 = a_1$$

$$\cdots$$

$$R_{k-1} = \left\lfloor \frac{R_{k-2}}{2} \right\rfloor = a_k \cdot 2, r_{k-1} = a_{k-2}$$

$$R_k = \left\lfloor \frac{R_{k-1}}{2} \right\rfloor = a_k$$

例如 $r=1023$，可得

$$1023=(1\ 111\ 111\ 111)_2。$$

令

$$\begin{aligned} r &= (r_k r_{k-1} \cdots r_1 r_0)_2 = r_k \cdot 2^k + r_{k-1}2^{k-1} + \cdots + r_1 2 + r_0 \\ &= ((\cdots((r_k \cdot 2 + r_{k-1})2 + r_{k-2})2 + \cdots)2 + r_1)2 + r_0 \end{aligned}$$

$$m^r = m^{((\cdots((r_k \cdot 2 + r_{k-1})2 + r_{k-2})2 + \cdots)2 + r_1)2 + r_0}$$

$$r_i \in (0,1), i = 0,1,2,\cdots,k, r_k = 1$$

令

$$m_1 = m^{r_k \cdot 2 + r_{k-1}} = \begin{cases} m^{r_k}, & r_{k-1} = 0 \\ m^{r_k} m, & r_{k-1} = 1 \end{cases}$$

$$m_2 = m^2 m^{r_{k-2}} = \begin{cases} m_1^2, & r_{k-1} = 0 \\ m_1^2 m, & r_{k-1} = 1 \end{cases}$$

$$\cdots$$

$$m_k = m^r = m_{k-1}^2 m_0^r = \begin{cases} m_{k-1}^2, & r_0 = 0 \\ m_{k-1}^2 m, & r_0 = 1 \end{cases}$$

可以总结求幂运算的规律，将 $r_k=1$，作 $m^1=m$。

从 r_{k-1} 开始 0 代表 S，1 代表 SM，其中 S 表示平方，M 表示乘以 m，例如：

$$(1\,010\,101)_2=85$$

除去第 1 个 1，后面 010101 代以

$$\underline{S}\ \underline{SM}\ \underline{S}\ \underline{SM}\ \underline{S}\ \underline{SM}$$

第 1 个 S 作 m^2，第 2 个 S 作 $(m^2)^2=m^4$，第 3 个 M 作 $(m^4)m=m^5$，第 4 个 S 作 $(m^5)^2=m^{10}$，第 5 个 S 作 $(m^{10})^2=m^{20}$，第 6 个 M 作 $m^{20}\cdot m=m^{21}$，第 7 个 S 作 $(m^{21})^2=m^{42}$，第 8 个 S 作 $(m^{42})^2=m^{84}$，第 9 个 M 作 $m^{84}\cdot m=m^{85}$。

我们感兴趣的是 r 和 m 都很大，特别是 r 特别大时，想节约计算的途径。

例如 m^{2731}：

$$2731=(101\,010\,101\,011)_2$$

可见其中 101 出现 3 次，预处理 $m^5=(m^2)^2\cdot m$；

$$m^{2731}=(((m^5)^{2^4}\cdot m^2)^{2^4}\cdot m^5)^2\cdot m$$

共作 11 次平方，4 次乘法。

若按传统办法：

$$\underset{0}{\underline{S}}\ \underset{1}{\underline{SM}}\ \underset{0}{\underline{S}}\ \underset{1}{\underline{SM}}\ \underset{0}{\underline{S}}\ \underset{1}{\underline{SM}}\ \underset{0}{\underline{S}}\ \underset{1}{\underline{SM}}\ \underset{1}{\underline{SM}}$$

共作 11 次平方 6 次乘法。

若 $r=2\,420\,027=(1\ \underline{011}\,\underline{011}\,\underline{111}\,\underline{110}\,\underline{100}\,\underline{111}\,\underline{011})_2$，窗口为 3 的有 100，111，011 预处理：

$$m^3=(m^2)\cdot m,m^4=(m^2)^2,m^7=(m^4)\cdot m^3$$

$$m^{2\,420\,027}=(((((m)^{2^3}\cdot m^3)^{2^3}\cdot m^3)^{2^3}\cdot m^7)^{2^3}\cdot m^4)^{2^5}\cdot m^2$$

共 23 次平方，8 次乘法。

若用传统方法应有

（S SM SM S SM SM SM SM SM S SM SM S SM S S SM SM SM S SM SM）

共 21 次平方 15 次乘法。

$$2\,420\,027=605\,007\times 3+605\,006$$

$$605\,007=(10010011101101001111)_2$$

$$605\,006=(10010011101101001110)_2$$

计算从左向右进行故

$$m^{2\,420\,027}=(((((((((((m^4)^{2^2}\cdot m^4)^2\cdot m^4)^2\cdot m^4)^2\cdot m^4)^4\cdot m^4)^2\cdot m^4)^4\cdot m^4)^2\cdot m^4)^2\cdot m^4)^2\cdot m^2$$

共作 16 次平方 10 次乘法。

(7) Barrett 归约：

已知 $N=(n_{2k-1}n_{2k-2}\cdots n_1n_0)_b$，$M=(m_{k-1}m_{k-2}\cdots k_1k_0)_b$，$m_{k-1}\neq 0$；求 $N(\bmod M)$，$\mu=\left\lfloor\frac{b^{2k}}{M}\right\rfloor$。

S1 $q_1 \leftarrow \left\lfloor \frac{N}{b^{k-1}} \right\rfloor, q_2 \leftarrow q_i\mu, q_3 \leftarrow \left\lfloor \frac{q_2}{b^{k+1}} \right\rfloor$。

S2 $r_1 \leftarrow N \pmod{b^{k+1}}, r_2 \leftarrow q_3 \cdot M \pmod{b^{k+1}}, r \leftarrow r_1 - r_2$。

S3 若 $r<0$，则做 $r \leftarrow r+b^{k+1}$。

S4 若 $r \geqslant m$，则做**始** $r \leftarrow r-m$，转 S4 **终**。

S5 输出 r。

例 7-5　$N=2789, M=97$。

$b=10, k=2, \mu=\left\lfloor \frac{10^4}{97} \right\rfloor=103$，

$q_1=\left\lfloor \frac{2789}{10} \right\rfloor=278, q_2=278\times 103=28\ 634$，

$q_3=\left\lfloor \frac{28\ 634}{10^3} \right\rfloor=28, r_1=2789 \pmod{10^3}=789$，

$r_2=28\times 97 \pmod{10^3}=2716 \pmod{10^3}=716$，

$r=789-716=73$。

例 7-6　$N=(313\ 221)_b=3651, M=(233)_b=47$，即 $x=3561, M=47, b=4, k=3$，$\mu=\left\lfloor \frac{46}{m} \right\rfloor=87=(1113)_b$，

$q_1=\left\lfloor \frac{(313\ 221)_b}{4^2} \right\rfloor=(3132)_b, q_2=(3132)_b \cdot (1113)_b=(10\ 231\ 302)_b$，

$q_3=(1023)_b, r_1=(3221)_b, r_2=(1023)_b \cdot (233)_b \pmod{b^4}=(3011)_b$，

$r=r_1-r_2=(210)_b, 2\times 4^2+4=32+4=36$。

$N \pmod{M}=36$。

(8) Montgomery 归约：

输入：整数 $m=(m_{n-1}m_{n-2}\cdots m_1m_0)_b$，$\gcd(m,b)=1, R=b^m, m'=-m^{-1} \pmod{b}$。

$T=(t_{2n-1}\cdots t_2t_1t_0)_b<mR$。

输出 $TR^{-1} \pmod{m}$。

S1 $A \leftarrow T, (A=(a_{2n-1}\cdots a_1a_0)_b), i \leftarrow 0$。

S2 若 $i \leqslant n-1$ 则作

始　$u_i \leftarrow a_im' \pmod{b}, A \leftarrow A+u_imb^i, i \leftarrow i+1$，转 S2 **终**。

S3 $A \leftarrow \frac{A}{b^n}$。

S4 若 $A \geqslant m$ 则 $A \leftarrow A-m$。

S5 输出(A)。

例 7-7　$m=72\ 639, b=10, R=10^5, T=7\ 118\ 368, n=5$，

$m=7263\times 10+9, 10=9+1$，

$1=10-(72\ 639-7263\times 10)=7264\times 10-72\ 639$，

$72\ 639\times(-1)\equiv 1 \pmod{10}$，

$m^{-1} \equiv (72\ 639)^{-1} \equiv -1 \pmod{10}$，

$m' = -m^{-1} \pmod{10} = 1$，$T \pmod{m} = 72\ 385$，

$TR^{-1} \pmod{m} = 39\ 796$，表 7-4 是 S2 的迭代过程。

表 7-4　S2 的迭代过程

i	$u_i = a_i m' \pmod{10}$	$u_i m b^i$	A
—	—	—	7 118 368
0	8	581 112	7 699 480
1	8	5 811 120	13 510 600
2	6	43 583 400	57 094 000
3	4	290 556 000	347 650 000
4	5	3 631 950 000	3 979 600 000

$i=0$，$u_0 a_0 m' \pmod{10} = 8$，$u_0 m = 72\ 639 \times 8 = 581\ 112$，

　　$A = 7\ 118\ 368 + 581\ 112 = 7\ 699\ 480$；

$i=1$，$a_1 = 8$，所以 $u_1 = 8$，$u_1 m \times 10^2 = 8 \times 72\ 639 \times 10 = 5\ 811\ 120$，

　　$A = 7\ 699\ 480 + 5\ 811\ 120 = 13\ 510\ 600$；

$i=2$，$u_2 = 6 \times 1 = 6$，$u_2 m \times b^2 = 6 \times 72\ 639 \times 100 = 43\ 583\ 400$，

　　$A = 13\ 510\ 600 + 43\ 583\ 400 = 57\ 094\ 000$；

$i=3$，$u_3 = 4$，$u_3 m \times (10)^3 = 4 \times 72\ 639 \times 1000 = 290\ 556\ 000$，

　　$A = 57\ 094\ 000 + 290\ 556\ 000 = 347\ 650\ 000$；

$i=4$，$u_4 = b_4 = 5$，$u_4 m \times 10\ 000 = 5 \times 72\ 639 \times 10\ 000 = 3\ 631\ 950\ 000$，

　　$A = 347\ 650\ 000 + 3\ 631\ 950\ 000 = 3\ 979\ 600\ 000$。

(9) Montgomery 乘法：

输入整数 $m = (m_{n-1} \cdots m_1 m_0)_b$，$x = (x_{n-1} \cdots x_1 x_0)_b$，$y = (y_{n-1} \cdots y_1 y_0)_b$，

$0 \leqslant x, y \leqslant m$，$R = b^n$，$\gcd(m, b) = 1$，$m' = -m^{-1} \pmod{b}$。

输出 $xyR^{-1} \pmod{m}$。

S1 $A \leftarrow 0$，$(A = (a_n a_{n-1} \cdots a_1 a_0)_b)$，$i \leftarrow 0$。

S2 若 $i \leqslant n-1$ 则作

始　$u_i \leftarrow (a_0 + x_i y_0) m' \pmod{b}$，$A \leftarrow \dfrac{(A + x_i y + u_i m)}{b}$，$i \leftarrow i+1$，转 S2 **终**。

S3 若 $A \geqslant m$，则 $A \leftarrow A - m$。

S4 输出(A)。

例 7-8　$m = 72\ 639$，$R = 10^5$，$x = 5792$，$y = 1229$，$n = 5$，

$m' = -m^{-1} \pmod{10}$，$xyR^{-1} \pmod{m} = 39\ 796$。

m 和 R 和前面例子一样，$xy = 7\ 118\ 368$，见表 7-5。

表 7-5　例 7-8 表

i	x_i	x_iy_0	u_i	x_iy	u_im	A
0	2	18	8	2458	581 112	58 357
1	9	81	8	11 061	581 112	65 053
2	7	63	6	8603	435 834	50 949
3	5	45	4	6145	290 556	34 765
4	0	0	5	0	363 195	39 796

现将本例的迭代过程详细说明如下。

$m=72\,639, R=10^5, b=10, x=5792, y=1229, n=5$，

$72\,639=7263\times10+9, 9=72\,639-7263\times10, 10=9+1$，

$1=10-1=10-(72\,639-7263\times10)=726\times10-72\,639$。

$-m\equiv-1(\text{mod }10)$，所以 $m^{-1}\equiv-m(\text{mod }10)-m^{-1}(\text{mod }10)=1$。

$i=0, x_0=2, y_0=9, x_0y_0=18, u_0=18\times1(\text{mod }10)\equiv8$

$x_0y=2\times1229=2458, u_0m=8\times72\,639=581\,112$

$$A=\frac{(2458+581\,112)}{10}=58\,357, b_0=7$$

$i=1, x_1=9, x_1y_0=9\times9=81, u_1=(7+81)(\text{mod }10)\equiv8$

$u_1m=8\times72\,639\equiv581\,112, x_1y=9\times1229=11\,061$

$$A=\frac{(58\,357+11\,061+581\,112)}{10}=65\,053$$

$i=2, x_2=7, x_2y_0=7\times9=63, u_2=(3+63)\times1(\text{mod }10)\equiv6$

$x_2y=7\times1229=8603, u_2m=6\times72\,639=435\,834$

$$A=\frac{(65\,053+8603+435\,834)}{10}=50\,949$$

$i=3, x_3=5, x_3y_0=5\times9=45, b_0=79$

$u_3=(9+45)\times1(\text{mod }10)=1, x_3y=5\times1229=6145$

$u_3m=4\times72\,639=290\,556$

$$A=\frac{(50\,946+6145+290\,556)}{10}=34\,765$$

$i=4, x_4=0, x_4y_0=0, x_4y=0, b_0=5$

$u_4=(5+0)(\text{mod }10)=5, u_4m=5\times72\,639=363\,195$

$$A=\frac{(34\,765+363\,165)}{10}=39\,796$$

(10) 求 gcd 的算法：

已知两个正整数 x 和 y，$x\geqslant y$，求 $\gcd\{x,y\}$。

S1 $g\leftarrow1$。

S2 若 x 和 y 都是偶数，则做**始** $x\leftarrow\frac{x}{2}, y\leftarrow\frac{y}{2}, g\leftarrow2g$ 转 S2 **终**。

S3 若 $x\neq 0$ 则做**始** A 若 x 是偶数则做**始** $x\leftarrow\frac{x}{2}$,转 A **终**。

B 若 y 是偶数则做**始** $y\leftarrow\frac{y}{2}$,转 B **终**。

$t\leftarrow\frac{|x-y|}{2}$,若 $x\geqslant y$ 则做 $x\leftarrow t$,否则 $y\leftarrow t$,转 S3。

S4 输出$(g\cdot y)$。

例 7-9 $x=1764,y=868$,求 gcd(1764,868)

gcd(1764,868)=28。

① $1764=4\times 441,868=4\times 217,g=2\times 2=4$。

② $112=7\times 16$。

③ $\frac{217-7}{2}=105,y\leftarrow 105$。

④ $\frac{105-7}{2}=49,y\leftarrow 49$。

⑤ $\frac{49-7}{2}=21,y\leftarrow 21$。

⑥ $\frac{21-7}{2}=7,y\leftarrow 7$。

⑦ $\frac{7-7}{2}=0,x\leftarrow 0$,见表 7-6。

表 7-6 例 7-9 表

x	1764	441	112	7	7	7	7	7	0
y	868	217	217	217	105	49	21	7	7
g	1	4	4	4	4	4	4	4	4

(11) 求 gcd 的扩展算法,已知 x 和 y,求 a,b,v,使 $ax+by=v,v=(x,y)$。

S1 $g\leftarrow 1$。

S2 若 x,y 都是偶数,则 $x\leftarrow\frac{x}{2},y\leftarrow\frac{y}{2},g\leftarrow 2g$ 转 S2。

S3 $u\leftarrow x,v\leftarrow y,A\leftarrow 1,B\leftarrow 0,C\leftarrow 0,D\leftarrow 1$。

S4 若 u 是偶数则作

始 $u\leftarrow\frac{u}{2}$,若 $A\equiv B\equiv 0(\bmod 2)$,则作**始** $A\leftarrow\frac{A}{2},B\leftarrow\frac{B}{2}$**终**;

否则**始** $A\leftarrow\frac{(A+y)}{2},B\leftarrow\frac{(B-x)}{2}$**终**,转 S4 **终**。

S5 若 v 是偶数则作

始 $v\leftarrow\frac{v}{2}$,若 $C\equiv D\equiv 0(\bmod 2)$,则作始 $C\leftarrow\frac{C}{2},D\leftarrow\frac{D}{2}$**终**;

否则**始** $C\leftarrow\frac{(C+y)}{2},D\leftarrow\frac{(D-x)}{2}$**终**,转 S5 **终**。

S6 若 $u \geqslant v$ 则作**始** $u \leftarrow u-v, A \leftarrow A-C, B \leftarrow B-D$ **终**；

否则作**始** $v \leftarrow v-u, C \leftarrow C-A, D \leftarrow D-B$ **终**。

S7 若 $u=0$ 则作**始** $a \leftarrow C, b \leftarrow D$，输出$(a,b,g \cdot v)$，结束**终**，否则转 S4。

例 7-10　$x=693, y=609$。

$693=609+84, 609=7\times 84+21$，

$84=4\times 21, \gcd(693,609)=21$，

$21=609-7\times 84=609-7\times(693-609)=8\times 609-7\times 693$，

(12) 指数运算：

$g \in G$，整数 $e \geqslant 1$，求 g^e。

S1 $A \leftarrow 1, S \leftarrow g$。

S2 若 $e \neq 0$ 则作

始　若 e 是奇数则作 $A \leftarrow A \cdot S$，

$e \leftarrow \left\lfloor \frac{e}{2} \right\rfloor$，

若 $e \neq 0$ 则 $S \leftarrow S \cdot S$

转 S2　**终**。

S3 输出(A)。

(13) 求 g^{283}，见表 7-7。

表 7-7　输出 g^{283}

A	1	g	g^3	g^8	g^{11}	g^{21}	g^{27}	g^{27}	g^{27}	g^{283}
e	283	141	70	35	17	8	4	2	1	0
S	g	g^2	g^4	g^8	g^{16}	g^{32}	g^{64}	g^{128}	g^{256}	—

$g \in G$，正整数 $e=(e_t e_{t-1} \cdots e_1 e_0)_2$：

S1 $A \leftarrow 1, i \leftarrow t$。

S2 若 $i \geqslant 0$ 则作

始　$A \leftarrow A \cdot A$，若 $e_i=1$ 则 $A \leftarrow A \cdot g, i \leftarrow i-1$，转 S2 **终**。

S3 输出(A)，见表 7-8。

表 7-8　输出 A

i	8	7	6	5	4	3	2	1	0
e_i	1	0	0	0	1	1	0	1	1
A	g	g^2	g^4	g^8	g^{17}	g^{35}	g^{70}	g^{141}	g^{285}

(14) 已知 g 及 $e=(e_t e_{t-1} \cdots e_1 e_0)_b, b=2^k, k \geqslant 1$，求 g^e。

S1 预处理：

$g_0 \leftarrow 1, i \leftarrow 1$

K 若 $i \leqslant 2^k-1$ 则作 $g_i \leftarrow g_{i-1} \cdot g, i \leftarrow i+1$ 转 K$(g_i=g^i)$。

S2 $A \leftarrow 1, i \leftarrow t$。

S3 若 $i \geqslant 0$ 则作

始　$A \leftarrow A^{2^k}, A \leftarrow A \cdot g_{e_i}, i \leftarrow i-1$,转 S3,**终**。

S4 输出(A)。

(15) 已知 g 和 $e=(e_t e_{t-1} \cdots e_1 e_0)_b, b=2^k, k \geqslant 1$。

S1 预处理:

$g_0 \leftarrow 1, g_1 \leftarrow g, g_2 \leftarrow g^2, i \leftarrow 1$。

K:若 $i \leqslant 2^k-1$ 作**始** $g_{2i+1} \leftarrow g_{2i-1} \cdot g_2, i \leftarrow i+1$,转 K **终**。

S2 $A \leftarrow 1, i \leftarrow t$。

S3 若 $i \geqslant 0$ 则作

始若 $e_i=0$ 则作**始** $A \leftarrow A^2, i \leftarrow i-1$ **终** 否则作

始寻找最长序列 $e_i e_{i-1} \cdots e_l$ 使 $i-l+1 \leqslant k$,且 $e_l=1$。

$A \leftarrow A^{2^{i-l+1}} \cdot g_{(e_i e_{i-1} \cdots e_l)_2}, i \leftarrow l-1$,转 S3 **终**。

S4 输出(A)。

7.3　离散对数

如果说 RSA 公钥密码不易被攻破是基于大数分解的困难,像 Elgamal 公钥密码的脱颖而出则基于离散对数的困难性。

问题的提出:已知 a 是一整数,$(a,n)=1$,r 是 mod n 的一个原根,求一整数 β,使 $a \equiv r^\beta \pmod n$。

若 p 是大素数,a 是$\{0,1,2,\cdots,p-1\}$中与 p 互素的数,即 a 是 mod p 的本原元素。已知 $a^x \pmod p \equiv B$,若倒过来假定给定 B 求 x,令

$x=b_0+b_1 2+b_2 2^2+\cdots+b_{n-1} 2^{n-1}$,

$a^x=a^{b_0} \cdot (a^2)^{b_1} \cdot (a^{2^2})^{b_2} \cdots (a^{2^{n-1}})^{b_{n-1}}$,

而且 $(a^{2^i})^{b_i}=\begin{cases} 1, & b_i=0, \\ a^{2^i}, & b_i=1。\end{cases}$

故 $a^2=a \cdot a$,

$a^{2^2}=a^2 \cdot a^2$,

$\cdots$

$a^{2^{n-1}}=a^{2n-2} \cdot a^{2n-2}$,

例如 $p=1823, a=5$,求 a^{375}。

$375=1+2+2^2+2^4+2^5+2^6+2^8=1+2+4+16+32+64+256$,

$5^{375}=5 \cdot 5^2 \cdot 5^4 \cdot 5^{16} \cdot 5^{32} \cdot 5^{64} \cdot 5^{256}$。

$5^2 \equiv 25 \pmod{1823}, 5^4 \equiv 625 \pmod{1823}$,

$5^8=(625)^2=309\,625 \equiv 503 \pmod{1823}$,

$5^{16} \equiv (503)^2 \equiv 1435 \pmod{1823}$,

$5^{32} \equiv (1435)^2 \equiv 2\ 059\ 225 \equiv 1058 \pmod{1823}$，

$5^{64} \equiv 42 \pmod{1823}$，

$5^{128} \equiv 1764 \pmod{1823}$，

$5^{256} \equiv 1658 \pmod{1823}$，

所以

$$5^{375} \equiv 5 \times 25 \times 625 \times 503 \times 1435 \times 1058 \times 42 \times 1658 \equiv 591 \pmod{1823}$$

这是已知 $x=375$，$a=5$，求 a^x，反过来已知 y，求 x，使 $y=a^x$ 就更不容易了，这就是所谓求离散对数的困难性。

7.4　求离散的 Baby-Step giant-step 算法

循环群 G 的阶为 n，α 是其生成元素，$\beta \in G$，求 $x=\log_\alpha \beta$。

S1 $m \leftarrow \lceil \sqrt{n} \rceil$。

S2 构造 (j, α^j) 表，$0 \leqslant j < m$，对表的第二个元素进行排序。

S3 计算 α^{-m}，$\gamma \leftarrow \beta$，$i \leftarrow 0$。

S4 若 $i < m$ 则作

始　(1) 检查若 γ 是表中的第二个元素；

(2) 若 $\gamma = \alpha^j$ 则作

始 $\gamma \leftarrow \gamma \cdot \alpha^{-m}$，输出 $(x = im + j)$，$i \leftarrow i+1$ 转 S4，**终**。

终　否则结束。

例 7-11　$p=113$，$\alpha=3$，α 是 Z_{113}^* 的生成元素，Z_{113}^* 的阶 $n=112$，令 $\beta=57$，$\log_3 57$ 计算如下。

(1) $m \leftarrow \lceil \sqrt{112} \rceil = 11$。

(2) 构造 $(j, \alpha^j \bmod 113)$ 表，如表 7-9 所示，其中 $0 \leqslant j < 11$。

表 7-9　例 7-11 表 1

j	0	1	2	3	4	5	6	7	8	9	10
$3^j \pmod{113}$	1	3	9	27	81	17	51	40	7	21	63

对表 7-8 的第二元素进行排序得表 7-10。

表 7-10　例 7-11 表 2

j	0	1	8	2	5	9	3	7	6	10	4
$3^j \pmod{113}$	1	3	7	9	17	21	27	40	51	63	81

(3) 计算 $\alpha^{-1} \equiv 3^{-1} \pmod{113} \equiv 38$，$\alpha^{-m} \equiv 38^{11} \pmod{113} \equiv 58$。

(4) $\gamma = \beta\alpha^{-mi} \pmod{113}$，$i=0,1,2,\cdots$ 直到有一数在第二行为止，得表 7-11。

表 7-11　例 7-11 表 3

i	0	1	2	3	4	5	6	7	8	9
$\gamma=57\cdot 58^i \pmod{113}$	57	20	100	37	112	55	26	39	2	3

前后因 $\beta\alpha^{9m}=3=\alpha^1$，$\beta=\alpha^{100}$，故$\log_3 57=100$。

$\alpha^{-11}\equiv 58 \pmod{113}$，

$57\cdot 58^i \pmod{113}\equiv 57\cdot(\alpha^{-11})^9\equiv 57\cdot\alpha^{-99}\pmod{113}$，

即 $\beta\cdot\alpha^{-99}\equiv\alpha$，$\beta=\alpha^{100}$。

7.5　Pohlig-Hellman 算法

输入：n 阶循环群 G 的生成元素 α 及一元素 $\beta\in G$。

输出：离散对数 $x=\log_\alpha\beta$。

S1 分解 $n=p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r}$，$l_i\geqslant 1$，$1\leqslant i\leqslant r$，$i\leftarrow 1$。

S2 若 $i\leqslant r$ 则作

　始　$\gamma\leftarrow 1$，$l_{-1}\leftarrow 0$，$\bar{\alpha}\leftarrow\alpha^{\frac{n}{q}}$，$j\leftarrow 0$。

　　SA：若 $j\leqslant\alpha_{j-1}$则作

　　　始（计算 $x_i=l_0+l_1p_1+\cdots+l_{\alpha_{i-1}}p_i^{\alpha_i-1}$，其中 $x\equiv x_i\pmod{p_i^{\alpha_i}}$）

　　　$\gamma\leftarrow 1$，$l_{-1}\leftarrow 0$，$\bar{\alpha}\leftarrow\alpha^{\frac{n}{q}}$，$j\leftarrow 0$。

　　　（计算 l_j）

　　　$\gamma\leftarrow\gamma\alpha^{l_{j-1}q^{j-1}}$，$\bar{\beta}\leftarrow(\beta\gamma^{-1})q^{\frac{n}{q^{j+1}}}$。

　　　计算 $l_j\leftarrow\log_{\bar{\alpha}}\bar{\beta}$，$j\leftarrow j+1$，转 SA 终，否则转 SB。

　　SB：$x_i\leftarrow l_0+l_1q+\cdots+l_{\alpha_{i-1}}q^{\alpha-1}$，$i\leftarrow i+1$，转 S2，**终**。

S3 利用 Gauss 算法计算 x，已知 $x\equiv x_i\pmod{p_i^{l_i}}$，$0<x\leqslant n-1$，$1\leqslant i\leqslant r$。

S4 输出 x。

例 7-12　$p=251$，$\alpha=71$，是 250 阶循环群的生成元素，$\beta=210$，$x=\log_{71}210$。

(1) $250=2\cdot 5^3$。

(2)（计算 $x\equiv x_1\pmod 2$）。

计算$\bar{\alpha}=\alpha^{\frac{n}{2}}\bmod p$，$\bar{\beta}=\beta^{\frac{n}{2}}\bmod p$：

① $\alpha^{125}\pmod 2\equiv 250$，$\beta^{125}\pmod 2\equiv 250$，

$x_1=\log_{250}250=1$。

② （计算 $x\equiv x_2\pmod{5^3}=l_0+l_15+l_25^2$）。

求$\bar{\alpha}=\alpha^{\frac{n}{5}}\bmod p$，$\bmod p$。

　$\alpha^1\equiv 77$，$\alpha^2\equiv 5041\equiv 21$，$\alpha^4\equiv 441\equiv 190$，$\alpha^8\equiv 36\,100\equiv 201$，

　$\alpha^{16}\equiv 42\,849\equiv 179$，$\alpha^{32}\equiv 32\,041\equiv 164$，$\alpha^{32+16+2}\equiv 164\times 179\times 21\equiv 616\,476\equiv 20$，

　$x\equiv\log_{71}210=197$。

补充：证$\bar{\alpha}=\alpha^{125}(\mathrm{mod}\ 251)\equiv 250$，$\bar{\beta}=\beta^{125}(\mathrm{mod}\ 251)\equiv 250$。

$\alpha=71$，$\beta=210$。

$(71)^2=5041\equiv 21$，

$(71)^4=441\equiv 190$，

$(71)^8=36\,100\equiv 207$，

$(71)^{16}=42\,849\equiv 179$，

$(71)^{32}=32\,041\equiv 164$，

$(71)^{64}=26\,896\equiv 39$，

$64+32+16+8+4+1=125$，

$(7!)^{125}\equiv 39\times 164\times 179\times 207\times 190\times 71$

$\equiv 6396\times 37\,053\times 13\,490\equiv 121\times 156\times 187\equiv 18\,876\times 187\equiv 51\times 187=9537\equiv 250$。

类似证 $\beta^{125}(\mathrm{mod}\ 251)=250$。

补充：$\bar{\beta}=\left(\dfrac{\beta}{\gamma}\right)^{\frac{n}{q^{j+1}}}=\left(\alpha^{x-l_0-l_1q-\cdots-l_{j-1}q^{j-1}}\right)^{\frac{n}{q^{j+1}}}$

$$=\left(\alpha^{\frac{n}{q^{j+1}}}\right)^{x_i-l_0-l_1q-\cdots-l_{j-1}q^{j-1}}=\left(\alpha^{\frac{n}{q^{j+1}}}\right)^{l_jq^j+\cdots+l_{\alpha-1}q^{\alpha-1-j}}$$

$$=\left(\alpha^{\frac{n}{q}}\right)^{l_j+\cdots+l_{\alpha-1}q^{\alpha-1-j}}=(\bar{\alpha})^{l_j}$$

最后一式之所以正确因又有指数 q，所以$\log_{\bar{\alpha}}\bar{\beta}$等于 l_j。

补充 S_A 内计算 $l_j\leftarrow\log_{\bar{\alpha}}\bar{\beta}$，例子是采用穷举法，实际上也可采用 7.4 节的方法。

7.6　Shank 法

Shank 算法比较高效，不仅速度快，而且需要的内存也较少。

$y\equiv a^x(\mathrm{mod}\ p)$，$0\leqslant x<n$，$n$ 是 a 的乘法周期，即 $a^n\equiv 1(\mathrm{mod}\ p)$，$0\leqslant x<n$。

Shank 算法的基本思想：运算在 $GF(p)$上进行。

(1) 选一 $d\approx\sqrt{n}$，$x=qd+r$，$0\leqslant r<d$，$q\leqslant\dfrac{x}{d}\approx\sqrt{n}$，$r<d\approx\sqrt{n}$。

(2) 建立一表格$(\lambda,\log_a\lambda)$，$\log_a\lambda=0,1,\cdots,d-1$，$\lambda$ 按顺序排序，以便检索。

(3) 由于假定 $y=a^x=a^{qd+r}$，所以 $y(a^{-d})^q=a^{qd+r}a^{-qd}=a^r$。

$$y(a^{-d})^q=y(a^{n-d})^q$$

计算 $y(a^{p-d})^q$，$q=0,1,2,\cdots$直到结果等于表中某 r，$r=\log_a x$，$x=qd+r$。

其中 $r=\log_a\gamma$。

Shank 算法：

S1 选 $d\approx\sqrt{n}$，$r\leftarrow 0$，$\gamma\leftarrow 1$。

S2 $(\lambda,\log_a\lambda)$进入表格。

S3 若 $r=d-1$ 则作

始　对表格中的 γ 进行排序转 S4　**终**。

否则作

始　$\gamma \leftarrow a\gamma, r \leftarrow r+1$，转 S2　**终**。

S4 计算 $A \leftarrow a^{n-d}, B \leftarrow y, q \leftarrow 0$。

S5 若存在(γ, r)，其中 $\gamma = B$，则作

始　$x \leftarrow qd + r$，输出 x 结束**终**。

否则作**始**　$B \leftarrow AB, q \leftarrow q+1$，转 S5 **终**。

Shank 算法如图 7-1 所示。

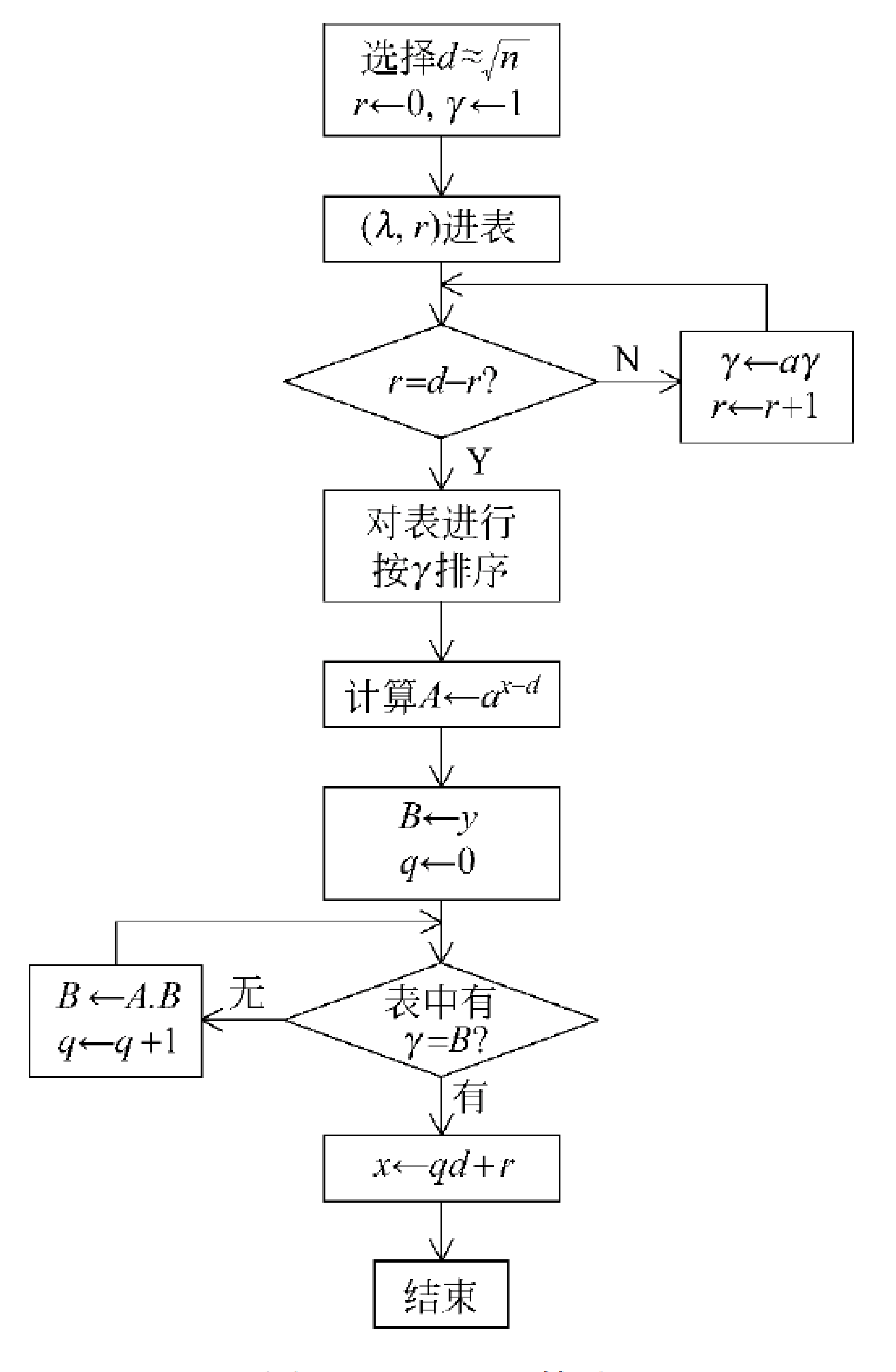


图 7-1　Shank 算法

例 7-13　在 $GF(23)$上求$\log_5 3$。5 的乘法周期 n 为 22，故 5 是 $GF(23)$的本原元素。$g = 5 \approx \sqrt{22}$，在 $GF(23)$上计算 $g = a^x, x = 1, 2, \cdots$, mod 23 有：

$5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv 2, 5^3 \equiv 10, 5^4 \equiv 4, 5^5 \equiv 20, 5^6 \equiv 8, 5^7 \equiv 17, 5^8 \equiv 16, 5^9 \equiv 11, 5^{10} \equiv 9, 5^{11} \equiv 22, 5^{12} \equiv 18, 5^{13} \equiv 21, 5^{14} \equiv 13, 5^{15} \equiv 19, 5^{16} \equiv 3$。

若用穷举法可得 $x = 16, g = 5^{16} \equiv 3 \bmod 23$ 或$\log_5 3 = 16$。

其实 $r = 0, 1, 2, \cdots, \gamma$ 分别对应的值依 γ 的顺序列于表 7-12 中。

表 7-12　例 7-13 表 1

γ	1	2	4	5	10
r	0	2	4	1	3

$5^{-d} = 5^{22-5} = 5^{17} = 15, A \leftarrow 15, q \leftarrow 0, y \leftarrow 3$，表中无 $\gamma \equiv 3 \equiv 5^{16}, 3 \times 15 \equiv 5^{16+17} \equiv 5^{33} \equiv 5^{11} \equiv 22, B \leftarrow 22, q \leftarrow 1$，表中无 $\gamma = 22$ 的行。

$22 \times 15 \equiv 5^{11+17} \equiv 5^6 \equiv 8, B \leftarrow 8, q \leftarrow 2$，表中无 $\gamma = 8$ 的行。

$8 \times 15 \equiv 5^{6+17} \equiv 5^{23} \equiv 5$，表中存在$(\gamma, r)$，其中 $\gamma = 5, r = 1, q = 3, x \equiv qd + r \equiv 3 \times 5 + 1 \equiv 16$，

下面介绍 n 可以因数分解时求离散对数的方法。

若 $n = n_1 n_2$，a 的乘法周期为 n，$a^n \equiv 1 \pmod n$，令 $a_1 \equiv a^{n_2}$ 的乘法周期为 n_1，$a_2 \equiv a^{n_1}$ 的乘法周期为 n_2，若 $b \equiv a^x, 0 \leqslant x \leqslant n$，

$x = x_2 n_1 + x_1, 0 \leqslant x_1 \leqslant n_1, 0 \leqslant x_2 \leqslant n_2$，

$b_1 = b^{n_2} = a^{x_2} = a^{x_2 n_1 n_2 + x_1 n_2}$，

由于 $a^{n_1 n_2} \equiv a^n \equiv 1 \pmod n$，

$b_1 = a^{x_2 n_1} = a_1^{x_1}, x_1 = \log_{a_1} b_1, b_2 = ba^{-x_1} = ba^{n-x_1}$，

$b_2 = a^{x_2 n_1 + x_1} a^{-x_1} = a^{x_2 n_1} = a_2^{x_2}, x_2 = \log_{a_2} b_2$，

故得 $n = n_1 n_2$ 时，求$\log_a b$ 的算法。

S1：$a_1 \leftarrow a^{n_2}, b_1 \leftarrow b^{n_2}$。

S2：求 $x_1 \leftarrow \log_{a_1} b_1$。

S3：$a_2 \leftarrow a^{n_1}, b_2 \leftarrow a^{n-x_1}$。

S4：求 $x_2 \leftarrow \log_a b_2$。

S5：$x \leftarrow x_2 n_1 + x_1$。

a 是 $GF(p)$ 上的本原元素，$y \equiv a^x \pmod p$，当 $p-1$ 有小素数时，求离散对数 $x = \log_a y$ 不困难，特别是 $GF(2^m)$，当 $m=127$ 时，$n=2^{127}-1$ 是素数，$\sqrt{n} \approx 10^{19}$。当 $m=521$ 时，$2^{521}-1$ 也是素数，$\sqrt{n} \approx 10^{28}$，可按下列方法求出 m，使满足 $29^m \equiv 30 \pmod{97}$。

先制作一表(见表 7-13)：$p_i \equiv 29^i \bmod 97, i=0,1,2,\cdots,9$。

表 7-13　例 7-13 表 2

i	0	1	2	3	4	5	6	7	8	9
p_i	1	29	65	42	54	14	18	37	6	77

设 $m=10j+i, 0 \leqslant i \leqslant 9$，

则 $29^i \equiv 30 \cdot 29^{-10j} \pmod{97}$，

$29^{-1} \equiv 87 \pmod{97}, 87^{10} \equiv 49 \pmod{97}$，

故 $29^i \equiv 30 \cdot 87^{10j} \pmod{97} \equiv 30 \cdot 49^i \pmod{97}$，

令 $j=0,1,2,\cdots,9$

$q_j \equiv 30 \cdot 49^8 \pmod{97}$，

与 $p_i \equiv 29^i \bmod 97$ 进行比较，

由于 $m<97, j \leqslant \left\lfloor \dfrac{97}{10} \right\rfloor = 9$，

不难发现 $i=5, j=4$ 有 $30 \cdot 49^4 \equiv 29^5 \pmod{97}$，

$m=4 \times 10+5=45$ 有 $29^{45} \equiv 30 \pmod{97}$。

7.7　数指标的算法

输入阶为 n 的循环群的生成元素 α 及一元素 $\beta \in G$，输出 $y=\log_\alpha \beta$。

S1 选一 G 的子集 $S=\{p_1,p_2,\cdots,p_t\}$，使 G 的元素的一部分可表示为 S 元素的乘积，$h \leftarrow 1$。

S2 若 $h \leqslant t+10$ 则作

始　A1 随机选一整数 $k, 0 \leqslant k \leqslant n$，计算 α^k，

若将 α^k 表示为 S 元素的乘积：

$\alpha^k = p_1^{c_1} p_2^{c_2} \cdots p_t^{c_t}, c_i \geqslant 0, i=1,2,\cdots,t$

成立，则作

始 $k \equiv c_1 \log_\alpha p_1 + c_2 \log_\alpha p_2 + \cdots + c_t \log_\alpha p_t$　　(*)

$h \leftarrow h+1$，转 S2 **终**，否则转 A1。

终 否则转 S3。

S3 从 $t+c$ 个方程组中求 $t \bmod n$ 个变数 $\log_\alpha p_i \bmod n$ 的值，$i=1,2,\cdots,t$，$h\leftarrow h+1$。

S4 若 $h\leqslant 2$ 则作

始 A2 随机选一整数 k，$0\leqslant k\leqslant n-1$，计算 $\beta\cdot\alpha^k$。

若将 $\beta\alpha^k$ 表示为 S 元素的乘积：

$$\beta\cdot\alpha^k=p_1^{d_1}\cdot p_2^{d_2}\cdot\cdots\cdot p_t^{d_t},d_i\geqslant 0,i=1,2,\cdots,t \qquad (**)$$

成立，则作

始 $h\leftarrow h+1$，转 S4 **终**，否则转 A2。

终。

S5 对(**)求对数得

$\log_\alpha\beta=(d_1\log_\alpha p_1+d_2\log_\alpha p_2+\cdots+d_t\log_\alpha p_t-k)\pmod n$。

计算 $y=(d_1\log_\alpha p_1+d_2\log_\alpha p_2+\cdots+d_t\log_\alpha p_t-k)\pmod n$，

输出 y。

数指标的算法要求找一个 G 元素的相对小的子集 S，如何找 S 是一种技巧。

例 7-14 $p=229$，$\alpha=6$，是 Z_{229}^* 的生成元素，$Z_{229}^*=\{a\mid 1\leqslant a\leqslant 228\}$ 群，$\beta=13$，求 $\log_6 13$ 如下：

(1) 取 $S=\{2,3,5,7,11\}$。

(2) $6^{100}\pmod{229}\equiv 180=2^2\cdot 3^2\cdot 5$，

$6^{18}\pmod{229}\equiv 176=2^4\cdot 11$，

$6^{12}\pmod{229}\equiv 165=3\cdot 5\cdot 11$，

$6^{62}\pmod{229}\equiv 154=2\cdot 7\cdot 11$，

$6^{143}\pmod{229}\equiv 198=2\cdot 3^2\cdot 11$，

$6^{206}\pmod{229}\equiv 210=2\cdot 3\cdot 5\cdot 7$。

(3) 这 6 个等式产生 6 个 S 元素的对数。

$100=2\log_6 2+2\log_6 3+\log_6 5\pmod{229}$，

$18=4\log_6 2+\log_6 11\pmod{229}$，

$12=\log_6 3+\log_6 5+\log_6 11\pmod{229}$，

$62=\log_6 2+\log_6 7+\log_6 11\pmod{229}$，

$143=\log_6 2+2\log_6 3+\log_6 11\pmod{229}$，

$206=\log_6 2+\log_6 3+\log_6 5+\log_6 11\pmod{229}$，

故 $\log_6 2=21$，$\log_6 3=208$，$\log_6 5=98$，$\log_6 7=107$，$\log_6 11=162$。

设 $k=77$，$\beta\alpha^k=13\cdot 6^{77}\pmod{229}\equiv 147\equiv 3\cdot 7^2$，因 $\beta\cdot\alpha^k=13\cdot 6^{77}\pmod{229}=147=3\cdot 7^2$，故

$$\log_6 13=(\log_6 3+2\log_6 7-77)\pmod{229}=117$$

例 7-15 在 $GF(2)$ 上的不可化约多项式 $f(x)=x^7+x+1$。

$GF(2^7)$ 域，阶为 128 的群 F_{27} 可以表示为 $GF(2)$ 上次方至多为 6 的多项式。

$\alpha=x$ 是 F_{27}^* 的生成元素，$F_{27}^*=\{a\in GF(2^7)\mid(a,f(x))=1\}$，

设 $\beta=x^4+x^3+x^2+x+1$，求 $\log_x\beta$ 的步骤如下。

$S=\{x,x+1,x^2+x+1,x^3+x+1,x^3+x^2+1\}$，$F_{2^7}^*$ 的阶 $=2^7-1=127$。

$x^{18}(\bmod f(x))=x^6+x^4=x^4(x+1)^2$，

$x^{105}(\bmod f(x))=x^6+x^5+x^4+x=x(x+1)^2(x^3+x^2+1)$，

$x^{72}(\bmod f(x))=x^6+x^5+x^3+x^2=x^2(x+1)^2(x^2+x+1)$，

$x^{45}(\bmod f(x))=x^5+x^2+x+1=(x+1)^2(x^3+x+1)$，

$x^{121}(\bmod f(x))=x^6+x^5+x^4+x^3+x^2+x+1=(x^3+x+1)(x^3+x^2+1)$，

令 $p_1=\log_x x$，$p_2=\log_x(x+1)$，$p_3=\log_x(x^2+x+1)$，$p_4=\log_x(x^3+x+1)$，

$p_5=\log_x(x^3+x^2+1)$，

$18\equiv 4p_1+2p_2(\bmod 127)$，

$105\equiv p_1+2p_2+p_3(\bmod 127)$，

$72\equiv 2p_1+2p_2+p_3(\bmod 127)$，

$45\equiv 2p_2+p_4(\bmod 127)$，

$121\equiv p_4+p_5(\bmod 127)$，

解上面 5 个未知数的方程组得

$$p_1=1,p_2=7,p_3=56,p_4=31,p_5=90$$

令 $k=66$，

$\beta\alpha^k\equiv(x^4+x^3+x^2+x+1)x^{66}(\bmod f(x))\equiv x^5+x^3+x\equiv x(x^2+x+1)^2$

$\log_x(x^4+x^3+x^2+x+1)=(p_1+2p_3-66)(\bmod 127)\equiv 47$

例 7-16　$p=541$，$g=2$，$p-1=540=2^2\cdot 3^3\cdot 5$，求 $2^m\equiv 345(\bmod 541)$。

$2^{\left(\frac{541-1}{2}\right)}\equiv 540(\bmod 541)$，

$2^{\left(\frac{54-1}{3}\right)}\equiv 125(\bmod 541)$，

$2^{\left(\frac{54-1}{5}\right)}\equiv 48(\bmod 541)$，

$S=(2,3,5,7)$，

$2^{14}\equiv 168\ 384\equiv 154=2\cdot 7\cdot 11(\bmod 541)$，

$2^{81}\equiv 294\equiv 2\cdot 3\cdot 7^2(\bmod 541)$，

$2^{207}\equiv 275\equiv 5^2\cdot 11(\bmod 541)$，

$2^{214}\equiv 35\equiv 5\cdot 7(\bmod 541)$，

$2^{300}\equiv 352\equiv 2^5\cdot 11(\bmod 541)$，

令 $m_1=\log_2 2$，$m_2=\log_2 3$，$m_3=\log_2 5$，$m_4=\log_2 7$，$m_5=\log_2 11$，

$2^{14}\equiv 2\cdot 7\cdot 11\equiv 2^{\log_2 2}\cdot 2^{\log_2 7}\cdot 2^{\log_2 11},\equiv 2^{m_1}\cdot 2^{m_4}\cdot 2^{m_5}(\bmod 541)$，

$14\equiv m_1+m_4+m_5(\bmod 540)$，

类似有 $81\equiv m_1+m_2+2m_4(\bmod 540)$，

$207\equiv 2m_3+m_4(\bmod 540)$，

$214\equiv m_3+m_4(\bmod 540)$，

$300\equiv 5m_1+m_5(\bmod 540)$，

联立解同余方程组得

$$m_1=1,m_2=104,m_3=496,m_4=258,m_5=295,$$

或 $2^1\equiv 2 \pmod{254}$，$2^{104}\equiv 3 \pmod{541}$，$2^{496}\equiv 5 \pmod{541}$，

$2^{258}\equiv 7 \pmod{258}$，$2^{295}\equiv 11 \pmod{541}$，

求 $2^m\equiv 345 \pmod{541}$，

$$345=3\cdot 5\cdot 23, 2^{12}\cdot 345\equiv 2^3\cdot 7 \pmod{541},$$

$$2^{13}\cdot 345\equiv 2^{13}\cdot 2^m\equiv 2^{13+m} \pmod{541},$$

$$2^3\cdot 7=2^3\cdot 2^{\log_2 7}=2^{3+\log_2 7}=2^{3\cdot\log_2 2+\log_2 7},$$

$$13+m=3m_1+m_4\equiv 3+258\equiv 261 \pmod{540}, m\equiv 248 \pmod{540},$$

即 $2^{248}\equiv 345 \pmod{541}$。

习　　题

1. 多位数乘、除编程。
2. 大数模幂运算编程。
3. Montgomery 乘法编程。
4. 求 $\gcd(x,y)$编程。
5. 求 a,b,v；使 $ax+by=v$，$v=\gcd(x,y)$编程。

第 8 章　椭圆曲线

椭圆曲线属代数几何学讨论的内容，近来发现它在密码学中有突出的应用，有报告指出，在椭圆曲线上建立一公钥密码，密钥长 150 比特，用每秒百万次的计算机进行分析需要 3.8×10^{10} 年，而一般密钥长 512 比特的 RSA 公钥仅需 3×10^{4} 年。

8.1　Weierstrass 方程

曲线 E(即椭圆曲线 E)：

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (a_1,a_2,a_3,a_4,a_6\in K)(*)$$

不妨假定域 K 是实数域 $\mathbf{R}$ 和有理数域 $\mathbf{Q}$。

引进变量置换

$$Y=y+\frac{1}{2}(a_1x+a_3),y=Y-\frac{1}{2}(a_1x+a_3),$$

代入(*)得

$$Y^2-(a_1x+a_3)Y+\frac{1}{4}(a_1^2x^2+2a_1a_3x+a_3^2)+a_1x\left[Y-\frac{1}{2}(a_1x+a_3)\right]$$
$$+a_3\left[Y-\frac{1}{2}(a_1x+a_3)\right]=x^3+a_2x^2+a_4x+a_6$$

令 $Y^2+\bar{a}_1xY+\bar{a}_3Y=x^3+\bar{a}_2x^2+\bar{a}_4x+\bar{a}_6$。

$$\bar{a}_1=(-a_1+a_1)=0,$$

$$\bar{a}_3=(-a_3+a_3)=0,$$

$$\bar{a}_2=a_2+\frac{1}{2}a_1^2-\frac{1}{4}a_1^2=a_2+\frac{1}{4}a_1^2,$$

$$\bar{a}_4=a_4-\frac{1}{2}a_1a_3+\frac{1}{2}a_1a_3+\frac{1}{2}a_1a_3=a_4+\frac{1}{2}a_1a_3,$$

$$\bar{a}_6=a_6-\frac{1}{4}a_3^2+\frac{1}{2}a_3^2=a_6+\frac{1}{4}a_3^2,$$

$$Y^2=x^3+\frac{1}{4}b_2x^2+\frac{1}{2}b_4x+\frac{1}{4}b_4,$$

$$b_2=4a_2+a_1^2,b_4=2a_4+a_1a_3,b_6=a_3^2+4a_6。$$

现在来考察椭圆曲线的可能图像。

例 8-1　$y^2=x^3-3x+3$。

曲线分解为关于 x 轴对称的两条曲线 $y=\pm\sqrt{x^3-3x+3}$。

以 $y=\sqrt{x^3-3x+3}$为例：

$$\frac{\mathrm{d}y}{\mathrm{d}x}=\frac{3x^2-3}{2\sqrt{x^3-3x+3}},令 y'=0,x=\pm1。$$

$$\frac{d^2y}{dx^2}=\frac{1}{2}\frac{d}{dx}\frac{3x^2-3}{\sqrt{x^3-3x+3}}=\frac{3(x^4-6x^2+2x-3)}{4\sqrt{x^3-3x+3}}$$

可以判断 $x=\pm1$ 有极值点，在 $(-1,1)$ 内有拐点，如图 8-1 所示。

例 8-2　$y^2=x^3-x$，$y=\pm\sqrt{x(x-1)(x+1)}$ 曲线在 $x=0$，$x=\pm1$，$y=0$。曲线在 $(0,1)$ 无定义如图 8-2 所示。

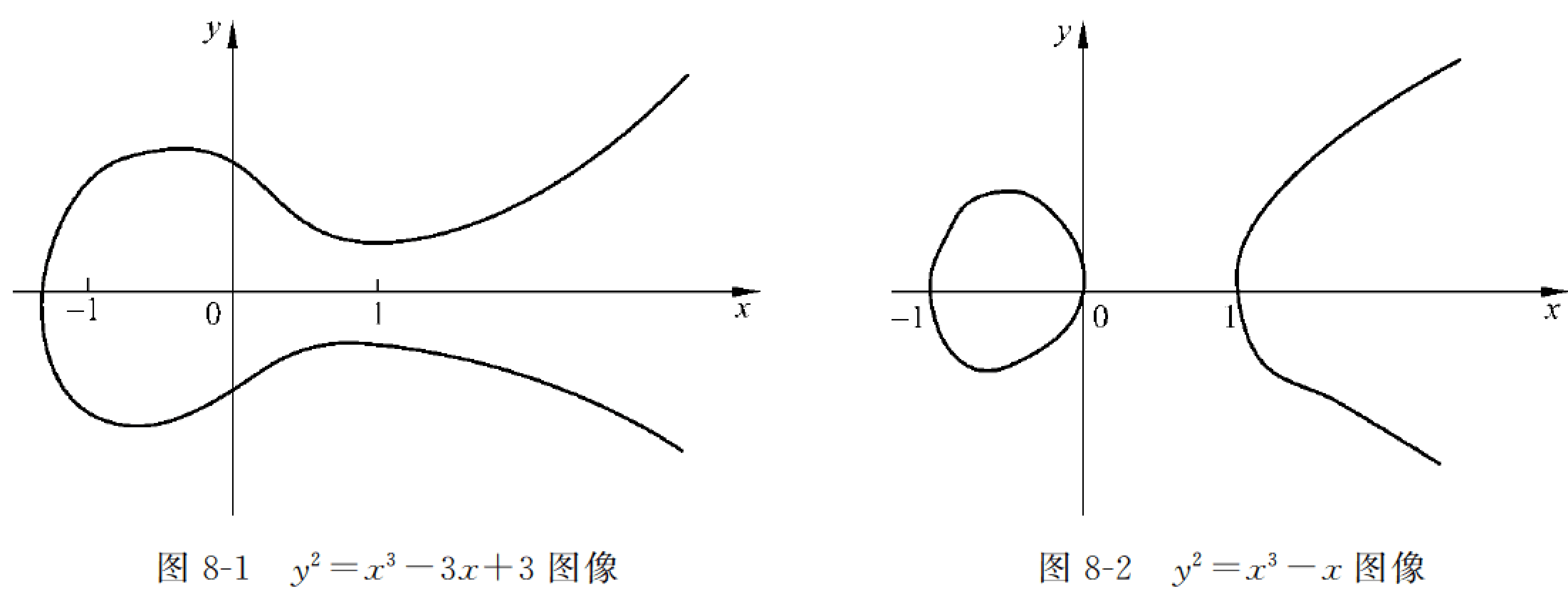


图 8-1　$y^2=x^3-3x+3$ 图像　　　图 8-2　$y^2=x^3-x$ 图像

例 8-3　$y^2=x^3+x^2$，$y=\sqrt{x^2(x-1)}$，$x=0$ 和 $x=-1$，$y=0$。

$\frac{dy}{dx}=\frac{3x^2+2x}{2\sqrt{x^3+x^2}}$，$\lim\limits_{x\to-1}\frac{dy}{dx}=+\infty$，如图 8-3 所示。

例 8-4　$y^2=x^3$，如图 8-4 所示。

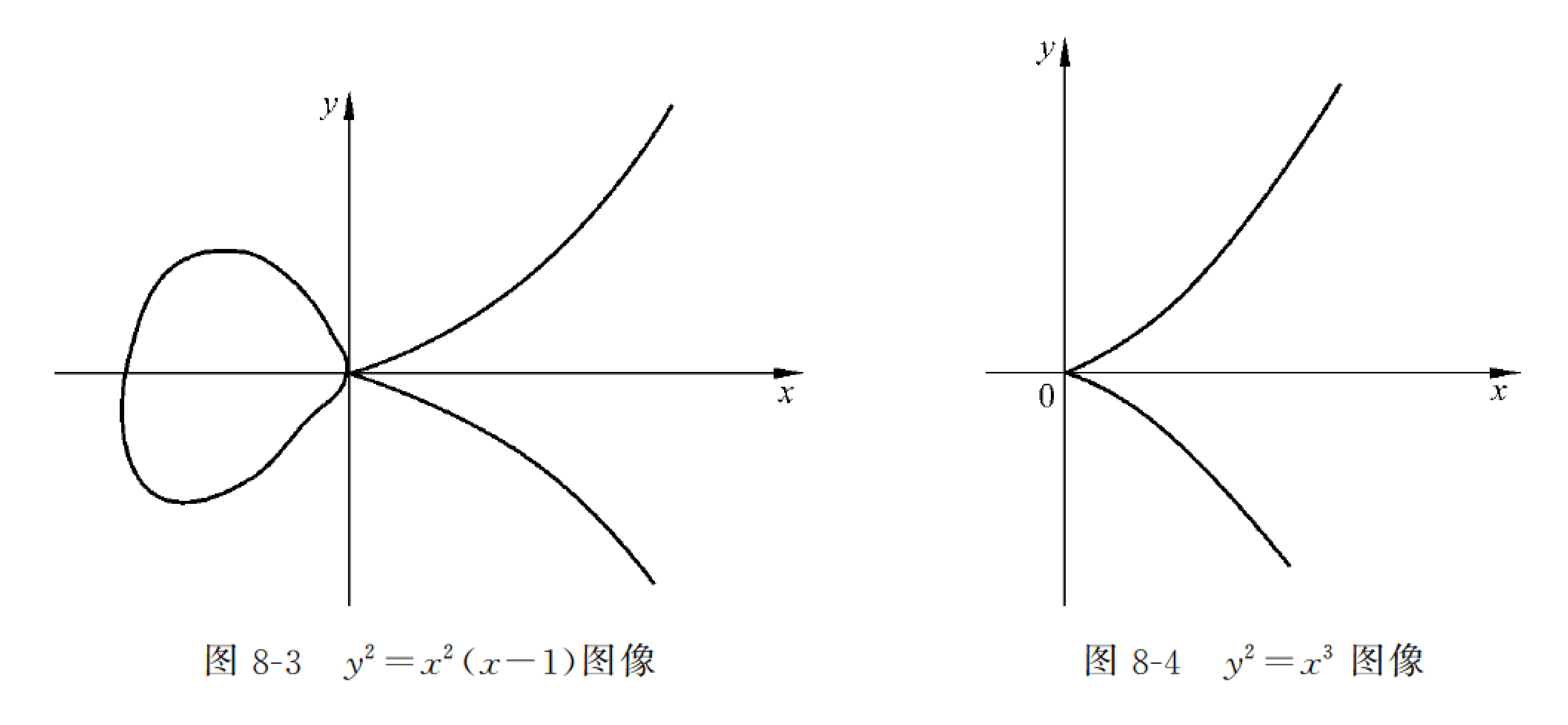


图 8-3　$y^2=x^2(x-1)$ 图像　　　图 8-4　$y^2=x^3$ 图像

8.2　判别式与结式

前面讨论了如何将 Weierstrass 方程转换成

$$E: y^2=x^3+ax+b$$

变换不改变奇异点的特性，奇异点是 $y^2=f(x)$ 中函数 $f(x)$ 和 $f'(x)$ 的公因子 $(x-a)$，即 $f(x)$ 含有 $(x-a)^2$ 的因式。

定理 8-1：$f(x)=f_0+f_1x+\cdots+f_mx^m$，

$g(x)=g_0+g_1x+\cdots+g_nx^n$,

$f_i\in K, i=1,2,\cdots,m; g_j\in K, j=1,2,\cdots,n$

$f(x)$和$g(x)$互素的充分必要条件是$(m+n)\times(m+n)$行列式:

$$R(f,g)=\begin{vmatrix} f_0 & f_1 & f_2 & \cdots & f_{m-1} & f_m & 0 & 0 & \cdots & 0 \\ 0 & f_0 & f_1 & \cdots & \cdots & f_{m-1} & f_m & & & \\ & & & & \cdots & \cdots & & & & \\ & & & & & f_0 & f_1 & \cdots & & f_m \\ g_0 & g_1 & g_2 & & \cdots & & g_n & \cdots & & 0 \\ & g_0 & g_1 & & \cdots & & g_{n-1} & g_n & \cdots & 0 \\ & & & & \cdots & \cdots & & & & \\ & & & & g_0 & g_1 & & \cdots & & g_n \end{vmatrix}\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m\text{ 行} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n\text{ 行}\end{matrix} \neq 0$$

$R(f,g)$称为$f(x)$和$g(x)$的结式。

证　先证$(f(x),g(x))\neq1$,即$f(x),g(x)$有公因式$a(x)$的充要条件是存在非零多项式$f_1(x)$和$g_1(x)$,使$g(x)f_1(x)=f(x)g_1(x)$,其中$f_1(x)$的次方小于m,$g_1(x)$的次方小于n。

因存在$d(x)=(f(x),g(x))$,$f_1(x)=\dfrac{f(x)}{d(x)}$,$g_1(x)=\dfrac{g(x)}{d(x)}$,

$\deg(f_1(x))<m$,$\deg(g_1(x))<n$,$f(x)g_1(x)=f_1(x)g(x)$。

反过来若存在非零多项式$f_1(x)$,$\deg(f_1(x))<m$,及$g_1(x)$,$\deg(g_1(x))<n$,$f_1(x)g(x)=g_1(x)f(x)$;则$(f(x),g(x))\neq1$。如若不然,从$f_1(x)g(x)=g_1(x)f(x)$可推出$f(x)\mid g(x)f_1(x)$,$(f(x),g(x))=1$,故$f(x)\mid f_1(x)$,与$\deg(f_1(x))<m$的假定矛盾。

令

$$f_1(x)=-a_0-a_1x-a_2x^2-\cdots-a_{m-1}x^{m-1}$$
$$g_1(x)=b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1},$$
$$f_1(x)g(x)=g_1(x)f(x)$$

可写成

$$(-a_0-a_1x-a_2x^2-\cdots-a_{m-1}x^{m-1})(g_0+g_1x+\cdots+g_nx^n)$$
$$=(b_0+b_1x+b_2x^2-\cdots-b_{n-1}x^{n-1})(f_0+f_1x+\cdots+f_mx^m)$$

可得关系式:

$$\begin{cases} b_0f_0+a_0g_0=0, \\ b_0f_1+b_1f_0+a_0g_1+a_1g_0=0, \\ \quad\vdots \\ b_{n-1}f_m+a_{m-1}g_n=0。\end{cases}$$

即$(b_0b_1\cdots b_{n-1}a_0a_1\cdots a_{m-1})[R(f,g)]=0$。

其中$[R(f,g)]$是行列式$R(f,g)$对应的方阵,上式有非零解:$b_0,b_1,\cdots,b_{n-1},a_0,a_1,\cdots,a_{m-1}$的充要条件是$R(f,g)=0$。

例 8-5　E: $y^2=x^3+ax+b$,$f(x)=x^3+ax+b$,$f'(x)=3x^2+a$。

$$R(f,f')=\begin{vmatrix} b & a & 0 & 1 & 0 \\ 0 & b & a & 0 & 1 \\ a & 0 & 3 & 0 & 0 \\ 0 & a & 0 & 3 & 0 \\ 0 & 0 & a & 0 & 3 \end{vmatrix}=b\begin{vmatrix} b & a & 0 & 1 \\ 0 & 3 & 0 & 0 \\ a & 0 & 3 & 0 \\ 0 & a & 0 & 3 \end{vmatrix}+a\begin{vmatrix} a & 0 & 1 & 0 \\ b & a & 0 & 1 \\ a & 0 & 3 & 0 \\ 0 & a & 0 & 3 \end{vmatrix}$$

$$=b\left[b\begin{vmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ a & 0 & 3 \end{vmatrix}+a\begin{vmatrix} a & 0 & 1 \\ 3 & 0 & 0 \\ a & 0 & 3 \end{vmatrix}\right]+a\left[a\begin{vmatrix} a & 0 & 1 \\ 0 & 3 & 0 \\ a & 0 & 3 \end{vmatrix}+\begin{vmatrix} b & a & 1 \\ a & 0 & 0 \\ 0 & a & 3 \end{vmatrix}\right]$$

$$=27b^2+9a^3$$

例 8-6　$y^2=x^3, a=b=0, 27b^2+9a^3=0$。

见 8.1 节的例 8-4,有奇异点。

8.3　椭圆曲线上的加法法则

E:$y^2=x^3+Ax+B$。　　(*)

设 $P(x_1,y_1),Q(x_2,y_2)$都是 E 上的有理点,$P\neq Q$,令 $P+Q=(x_3,y_3)$,连 PQ 的直线交 E 于 R 点,R 也是 E 上的有理点,R 关于 x 轴对称的点即 $P+Q$。

这里所谓有理点是指它的坐标是属于域 K 的有理式。

$P=Q$ 时,P 点的切线交 E 于 R 点,R 点关于 x 轴的对称点便是 $2P$。

过 $P(x_1,y_1),Q(x_2,y_2)$的直线方程设为

$$y=mx+b, m=\frac{y_2-y_1}{x_2-x_1}, b=y_1-mx_1=y_2-mx_2,$$

代入(*)得

$$x^3-m^2x^2+(a-2mb)x+(B-b^2)=0,$$
$$(x-x_1)(x-x_2)(x-x_3)=0,$$
$$x_1+x_2+x_3=m^2$$

利用根与系数关系求得 $x_3=m^2-(x_1+x_2), y_3=m(x_3-x_1)+y_1$,

故 $P\neq Q$ 时

$$\begin{cases} x_3=m^2-x_1-x_2, \\ y_3=m(x_3-x_1)+y_1, \end{cases}\quad m=\frac{y_2-y_1}{x_2-x_1}$$

例 8-7　$y^2=x^3+17, P_1=(-1,4), P_2=(2,5)$,求 $P_1+P_2=P_3(x_3,y_3)$,过 P_1P_2 的直线方程为 $y=mx+b, m=\frac{5-4}{2-(-1)}=\frac{1}{3}, b=5-\frac{2}{3}=4\frac{1}{3}=\frac{13}{3}$,过 P_1P_2 的直线方程为 $y=\frac{1}{3}x+\frac{13}{3}$。

代入 $y^2=x^3+17$ 得

$$\left(\frac{1}{3}x+\frac{13}{3}\right)^2=x^3+17, x^3-\frac{1}{9}x^2-\frac{26}{9}x-\left(\frac{169}{9}-17\right)=0,$$

$x^3-\frac{1}{9}x^2-\frac{26}{9}x-\frac{16}{9}=0$，

$x_1+x_2+x_3=-\frac{1}{9}$，

$x_3=-\frac{1}{9}-1=-\frac{10}{9}$，

$\frac{1}{3}\left(-\frac{10}{9}\right)+\frac{13}{3}=\frac{107}{27}$，

$P_1+P_2=P_3\left(-\frac{10}{9},-\frac{107}{27}\right)$。

例 8-8　$y^2=x^3+17, P_1=(-1,4)$，求 $2P$。

$2y\frac{\mathrm{d}y}{\mathrm{d}x}=3x^2\ \frac{\mathrm{d}y}{\mathrm{d}x}=\frac{3x^2}{2y}\Big|_{(-1,4)}=\frac{3}{8}$，过$(-1,4)$点的切线方程：

$$y-4=\frac{3}{8}(x+1), y=\frac{3}{8}x+\frac{35}{8}$$

代入 $y^2=x^3+17$，

$$\left(\frac{3}{8}x+\frac{35}{8}\right)^2=x^3+17, x^3-\frac{9}{64}x^2-\frac{210}{64}x-\frac{1225}{64}+17=0,$$

$$x^3-\frac{9}{64}x^2-\frac{210}{64}x-\frac{137}{64}=0,$$

设切线：$y=\frac{3}{8}+\frac{35}{8}$交 E 于(x^*,y^*)，

$-\frac{9}{64}=-2+x^*, x^*=-\frac{9}{64}+2=\frac{119}{64}$，

$y^*=\frac{3}{8}\cdot\frac{119}{64}+\frac{35}{8}=\frac{357}{512}+\frac{35}{8}=\frac{2597}{512}$，

$2P=\left(\frac{119}{64},-\frac{2597}{512}\right)$。

例 8-9　$y^2+y=x^3-x^2, P=(1,0)$，求 $2P,3P,4P$。

令 $y=\eta-\frac{1}{2}, x=\xi, \left(\eta-\frac{1}{2}\right)^2+\left(\eta-\frac{1}{2}\right)=\xi^3+\xi^2$，

$\eta^2=\xi^3-\xi^2+\frac{1}{4}, P=\left(1,\frac{1}{2}\right)$，

问题变成 $\eta^2=\xi^3-\xi^2+\frac{1}{4}, P=\left(1,\frac{1}{2}\right)$，求 $2P,3P,4P$。

(1) 过$\left(1,\frac{1}{2}\right)$引切线方程 $\eta=m\xi+b$，

又 $\eta\frac{\mathrm{d}\eta}{\mathrm{d}\xi}=3\xi^2-2\xi, \frac{\mathrm{d}\eta}{\mathrm{d}\xi}=\frac{3\xi^2-2\xi}{2\eta}$

$m=\frac{3\xi^2-2\xi}{2\eta}\Big|_{\left(1,\frac{1}{2}\right)}=1, b=-\frac{1}{2}, \eta=\xi-\frac{1}{2}$，

$\left(\xi-\frac{1}{2}\right)^2=\xi^3-\xi^2+\frac{1}{4}$，

$\xi^3-2\xi^2+\xi=0$，

$2+\xi_2=2, \xi_2=0, \eta=\xi-\frac{1}{2}=-\frac{1}{2}$，

$2P=\left(0,\frac{1}{2}\right)$。

(2) 过$\left(1,\frac{1}{2}\right)$和$\left(0,\frac{1}{2}\right)$，引直线方程 $\eta=m\xi+b, m=0, b=-\frac{1}{2}, \eta=\frac{1}{2}, \left(\frac{1}{2}\right)^2=\xi^3-\xi^2+\frac{1}{4}, 2+\xi_3=1, \xi_3=-1, \eta=\frac{1}{2}, 3P=\left(-1,-\frac{1}{2}\right)$。

(3) $2(2P)=4P$，引$\left(0,\frac{1}{2}\right)$的切线方程 $y=mx+b$，

$m=\left.\frac{3\xi^2-2\xi}{2\eta}\right|_{\left(0,\frac{1}{2}\right)}=0, \eta=\frac{1}{2}$，

$\left(\frac{1}{2}\right)^2=\xi^3-\xi^2+\frac{1}{4}, \xi^3-\xi^2=0$，

$0+\xi_4=1, \xi_4=1, \eta=\frac{1}{2}$，

$4P=\left(1,-\frac{1}{2}\right)$。

(4) $\left(1,\frac{1}{2}\right)$和$\left(-1,-\frac{1}{2}\right)$，连线方程 $\eta=m\xi+b$，

$m=\frac{1}{2}, b=0, \eta=\frac{1}{2}\xi$。

$\left(\frac{1}{2}\xi\right)^2=\xi^3-\xi^2+\frac{1}{4}$。

$\xi^3-\frac{5}{4}\xi^2+\frac{1}{4}=0$。

$1+(-1)+\xi_4=1, \xi_4=1, \eta=\frac{1}{2}$。

$4P=\left(1,-\frac{1}{2}\right)$。

例 8-10 $y^2=x^3-36x, P=(-3,9), Q=(-2,8)$，求 $P+Q$ 及 $2P$。

(1) PQ 连线 $y=mx+b, m=\frac{9-8}{-3+2}=-1, b=6$，以 $y=-x+6$ 代入 $y^2=x^3-36x$ 得

$(-x+6)^2=x^3-36x, x^3-x^2-24x+36=0$，

$(x+3)(x+2)(x-x_2)=0, 3+2-x_2=-1, x_2=6$，

$y_2^2=36\times6-36\times6=0, y_2=0$，

$P+Q=(6,0)$。

(2) $\frac{\mathrm{d}y}{\mathrm{d}x}=\left.\frac{3x^2-36}{2y}\right|_{(-3,9)}=\frac{27-36}{18}=-\frac{1}{2}$，

过 P 点的切线方程：$y=-\frac{x}{2}+\frac{15}{2}$和 E 交于(x_3, y_3)，将 $y=-\frac{x}{2}+\frac{15}{2}$代入 E：

$$\left(-\frac{x}{2}+\frac{15}{2}\right)^2=x^3-36x, x^3-\frac{1}{4}x^2+\left(\frac{15}{2}-36\right)x-\frac{225}{4}=0,$$

$$-6+x^3=\frac{1}{4}, x^3=6\frac{1}{4}, y_3=\frac{1}{2}\cdot\frac{25}{4}+\frac{15}{2}=\frac{35}{8},$$

$$2P=\left(\frac{25}{4},-\frac{35}{8}\right)。$$

例 8-11　$y^2+y=x^3+x^2, P=(0,0)$，求 $2P,3P,4P$。

令 $\eta-\frac{1}{2}=y, \xi=x, \eta=y+\frac{1}{2}$，

$\left(\eta-\frac{1}{2}\right)^2+\left(\eta-\frac{1}{2}\right)=\xi^3+\xi^2, \eta^2=\xi^3+\xi^2+\frac{1}{4}, P=\left(0,\frac{1}{2}\right)$。

(1) $2\eta\frac{d\eta}{d\xi}=3\xi^2+2\xi, \left.\frac{d\eta}{d\xi}\right|_{\left(0,\frac{1}{2}\right)}=\frac{3\xi^2+2\xi}{2\eta}=0$，

切线方程 $\eta=\frac{1}{2}$，

$\frac{1}{4}=\xi^3+\xi^2+\frac{1}{4}, \xi^3+\xi^2=\xi^2(\xi+1)=0$，

$2P=(\xi_2,\eta_2)=\left(-1,-\frac{1}{2}\right)$。

(2) $\left(-1,-\frac{1}{2}\right)$和$\left(0,\frac{1}{2}\right)$连线方程 $\eta=\xi+\frac{1}{2}$，

$\left(\xi+\frac{1}{2}\right)^2=\xi^3+\xi^2+\frac{1}{4}, \xi^3-\xi=0, \xi(\xi-1)(\xi+1)=0$，

$\xi_3=1, \eta=1+\frac{1}{2}=\frac{3}{2}, 3P=\left(1,-\frac{3}{2}\right)$。

(3) 求 $4P=(\xi_4,\eta_4)$。从 $2P=\left(-1,-\frac{1}{2}\right)$，引切线方程：$\eta=m\xi+b$，

$$m=\frac{d\eta}{d\xi}=\left(\frac{3\xi^2+2\xi}{2\eta}\right)_{\left(-1,-\frac{1}{2}\right)}=\frac{3-2}{-1}=-1, b=-\frac{3}{2},$$

切线方程 $\eta=-\xi-\frac{3}{2}$，代入 $\eta^2=\xi^3+\xi^2+\frac{1}{4}$，

$$\left(-\xi-\frac{3}{2}\right)^2=\xi^3+\xi^2+\frac{1}{4}, \xi^3+3\xi-2=0,$$

$$-2+\xi_4=0, \xi_4=2, \eta=-2-\frac{3}{2}=-\frac{7}{2}=-3\frac{1}{2},$$

$$4P=\left(2,3\frac{1}{2}\right)。$$

(4) $P+3P=4P, P=\left(0,\frac{1}{2}\right), 3P=\left(1,-\frac{3}{2}\right)$，$P$ 和 $3P$ 连线方程 $\eta=-2\xi+\frac{1}{2}$，

$$\left(-2\xi+\frac{1}{2}\right)^2=\xi^3+\xi^2+\frac{1}{4}, \xi^3-3\xi^2+2\xi=0,$$

$$\xi(\xi^2-3\xi+2)=\xi(\xi-2)(\xi-1)=0,$$

$$\xi_4=2,$$

$$4P=\left(2,3\ \frac{1}{2}\right)$$ 。

8.4 椭圆曲线上的无穷远点及有限域上的椭圆曲线

在椭圆曲线上的无穷远点用 O 表示,对 $P,Q\in E$ 有:

(1) $O+P=P,P+O=P$。

(2) $-O=O$。

(3) 若 $Q=-P,P+Q=O$。

椭圆曲线关于加法构成交换律,下面将证明此重要结果,O 便是关于群的单位。

例 8-12 $y^2=x^3+x+6,K=GF(11)$。

$x=1,y^2=1+1+6=8,y\notin GF(11)$,

$x=2,y^2=8+2+6=16,y=4\in GF(11),(2,4)\in GF(11)$。

$(2,4)$关于 x 轴的对称点$(2,-4)=(2,7)\in E$。

$x=3,y^2=27+3+6=36,y=6\in GF(11),(3,6)\in E,(3,-6)=(3,5)\in E$。

$x=4,y^2=64+4+6=74\equiv 8,y\notin GF(11)$。

$x=5,y^2=125+5+6=136\equiv 4,y=2\in GF(11),(5,2)\in E,(5,-2)=(5,9)\in E$。

$x=6,y^2=216+6+6=228\equiv 8,y\notin GF(11)$。

$x=7,y^2=343+7+6=356\equiv 4,y=2\in GF(11),(7,2)\in E,(7,-2)=(7,9)\in E$。

$x=8,y^2=512+8+6=526\equiv 9,y=3\in GF(11),(8,3)\in E,(8,-3)=(8,8)\in E$。

$x=9,y^2\equiv 729+9+6=7\equiv 7,y\notin GF(11)$。

$x=10,y^2=1000+10+6=1016\equiv 4,y=2\in GF(11),(10,2)\in E,(10,-2)=(10,9)\in E$。

总之:

$E(GF(11))=\{O,(2,4),(2,7),(3,5),(3,6),(5,2),(5,9),(7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$。

例 8-13 $y^2=x^3+x+6,K=GF(11)$。

(1) 求$(2,4)+(3,5)$。

$(2,4)$和$(3,5)$连线的方程 $y=mx+b$,其中

$m=\dfrac{5-4}{3-2}=1,b=2,y=x+2$。

代入 $y^2=x^3+x+6$ 得$(x+2)^2=x^3+x+6,(x+2)^2=x^3-x^2-3x+2=0$,

$(x-2)(x-3)(x-x^*)=0$,

$2+3+x^*=1,x^*=-4\equiv 7,(7,9)\in E,(7,-9)=(7,2)\in E$,

所以$(2,4)+(3,5)=(7,-9)$。

(2) 求$(2,4)+(5,9)$。

$m=\dfrac{9-4}{5-3}=\dfrac{5}{3}=3^{-1}\times 5,GF(11)$关于乘法 $3^{-1}=4,11=3\times 3+2,2=11-3\times 3,3=2+1,1=3-2=3-(11-3\times 3)=4\times 3-11$。

故 $3^{-1}(\bmod 11)=3$。

$m=4\times5=20\equiv9\ y=9x+b, b=8$,

$(mx+b)^2=x^3+x+6$。

$x^3-m^2x-(2mb+1)x-b^2+6=0$,

$(x-2)(x-5)(x-x^*)=-m^2$,

$x^*=m^2-2-5=81-2-5=74\equiv8 \pmod{11}$。

$y^*=9\times8+8=80\equiv3, (8,3)\in E$。

$(8,-3)=(8,8)\in E, (2,4)+(5,9)=(8,8)$。

(3) 求 2(2,4)。

$$2y\frac{\mathrm{d}y}{\mathrm{d}x}=3x^2+1, \frac{\mathrm{d}y}{\mathrm{d}x}=\left.\frac{3x^2+1}{2y}\right|_{(2,4)}=\frac{13}{8}=8^{-1}\times13,$$

$8^{-1}\equiv7 \pmod{11}, m=91\equiv3 \pmod{11}$。

$y=3x+b, b=-1=9$。

$(3x+b)^2=x^3+x+6, x^3-9x^2+(1-6b)x-b^2+6=0$,

$(x-2)^2(x-x^*)=0, -x^*-4=-9, x^*=9-4\equiv5$,

$y^*=3\times5+9=24=2, 2(2,4)=(5,9)$。

例 8-14　$E: y^2=x^3+x+4, K=GF(23)$。

① $x=0, y^2=4, y=2\in GF(23), (0,2)\in E, (0,-2)=(0,21)\in E$。

② $x=1, y^2=6, 11^2=121\equiv6 \pmod{23}$,所以 $y=\pm11, (1,11)\in E, (1,-11)=(1,12)\in E$。

③ $x=3, y^2=27+3+4=34\equiv11, y\notin GF(23)$。

④ $x=4, y^2=64+4+4=72\equiv3, y\notin GF(23)$。

⑤ $x=5, y^2=125+5+4=134\equiv19, y\notin GF(23)$。

⑥ $x=6, y^2=216+6+4=226\equiv19, y\notin GF(23)$。

⑦ $x=7, y^2=343+7+4=354\equiv9, y=3\in GF(23), (7,3)\in E, (7,-3)=(7,20)\in E$。

⑧ $x=8, y^2=512+8+4=524\equiv18, 8^2=64\equiv8, (8,8)\in E, (8,-8)=(8,15)\in E$。

⑨ $x=9, y^2=927+9+4=742\equiv6, 11^2=121=5\times23+6, (6,11)\in E, (6,-11)=(6,12)\in E$。

⑩ $x=10, y^2=1000+10+4=1014\equiv2, y=5, 5^2=25\equiv2, (10,5)\in E, (10,-5)=(10,18)\in E$。

⑪ $x=11, y^2=1331+11+4=1349\equiv12, 9^2=81\equiv12$,故 $(11,7)\in E, (10,-7)=(11,14)\in E$。

其他不一一列举,还有(13,11),(13,12),(14,5),(14,18),(15,6),(15,17),(17,9),(17,14),(18,9),(18,14),(22,5),(22,19),O。

例 8-15　$y^2=x^3+x+4, K=GF(23), P=(0,2)$,求 $KP, k=2,3,\cdots,29$。

$$m=\left.\frac{3x^2+1}{2y}\right|_{(0,2)}=\frac{1}{4}=4^{-1}\equiv6, y=6x+b, b=2,$$

$y=6x+2$,

$(6x+2)^2=x^3+x+4, x^3-36x^2-23x=0$,

$x^3-13x^2=0$，$x^2(x-13)=0$，$x^*=13$。

$y^*=6x^*+2=80\equiv 11$。

$(13,11)\in E$，$(13,-11)=(13,12)\in E$，$2P=(13,-11)=(13,12)$。

$3P=(11,9)$，$4P=(1,12)$，$5P=(7,20)$，$6P=(7,11)$，$7P=(15,16)$，$8P=(14,5)$，$9P=(4,7)$，$10P=(22,15)$，$11P=(10,5)$，$12P=(17,9)$，$13P=(8,15)$，$14P=(18,9)$，$15P=(18,14)$，$16P=(8,8)$，$17P=(17,14)$，$18P=(10,18)$，$19P=(22,18)$，$20P=(4,16)$，$21P=(14,18)$，$22P=(15,17)$，$23P=(9,12)$，$24P=(7,3)$，$25P=(1,11)$，$26P=(11,14)$，$27P=(13,11)$，$28P=(0,21)$，$29P=O$。

例 8-16　$y^2=x^3+x+4$，$K=GF(23)$，$P_1=(4,7)$，$P_2=(13,11)$：

(1) P_1+P_2。

(2) $2P_1$。

① 过 P_1 和 P_2 的直线方程：$y=mx+b$，

$m=\dfrac{11-7}{13-4}=\dfrac{4}{9}=9^{-1}\times 4$，

$23=2\times 9+5$，$9=5+4$，$5=4+1$，

$1=5-4=5-(9-5)=2\times 5-9=2\times(23-2\times 9)-9=2\times 23-5\times 9$，

$9^{-1}(\text{mod } 23)=-5\equiv 18(\text{mod } 23)$。

直线方程 $y=18\times 4x+b=72x+b=3x+b$，

$(3x+b)^2=x^3+x+4$，

$x^3-9x^2-(66-1)x+(4-b)=0$，

$4+13+x^*=9$，$x^*=9-17=-8\equiv 15(\text{mod } 23)$，

$y^*=-3(4-15)+7=33+7=40=17$。

$P_1+P_2=(15,-17)=(15,6)$。

② 令 $2P_1=(x^*,y^*)$，

过 P_1 点引切线方程 $y=mx+b$，

$m=\dfrac{\mathrm{d}y}{\mathrm{d}x}=\dfrac{3x^2+1}{2y}\Big|_{(4,7)}=\dfrac{49}{14}=14^{-1}\times 49=14^{-1}\times 3$。

$23=14+9$，$14=9+5$，$9=5+4$，$5=4+1$，

$1=5-4=5-(9-5)=2\times 5-9=2\times(14-9)-9=2\times 14-3\times 9=2\times 14-3(23-14)=5\times 14-3\times 23$。

$14^{-1}(\text{mod } 23)=5$，$m=5\times 3=15$。

令切线交 E 于 (ξ,η)，切线方程 $y=15x+b$，

$b=16$，$y=15x+16$，

$(15x+16)^2=x^3+x+4$，

$x^3-225x^2-(480-1)x-256+4=0$，

$x^3-18x^2-19x-22=0$，

$2\times 4+\xi=18$，$\xi=10$，$\eta=15\times 10+16=166\equiv 5$，

$2P_1=(10,-5)=(10,18)$。

8.5 $GF(2^k)$上的椭圆曲线

Weierstrass 方程

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$$

由坐标变换对不同的域的特征简化为：

(1) $\mathrm{char}(K)=2$，

E：$y^2+ay=x^3+bx+c$，

E：$y^2+ay=x^3+ax^2+c$，

(2) $\mathrm{char}(K)=3$，

E：$y^2=x^3+ax^2+bx+c$，

(3) $\mathrm{char}(K)>3$，

E：$y^2=x^3+ax+b$，

定义 $d_2=a_1^2+4a_2, d_4=2a_4+a_1a_3, d_6=a_3^2+4a_6$，

$d_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2$

$c_4=d_2^2-24d_4, \Delta=-d_2^2d_8-8d_4^3-27d_6^2+9d_2d_4d_6$

$j(E)=\dfrac{c_4^2}{\Delta}$

Δ 称为 Weierstrass 方程的判别式：

若 $\Delta\neq 0$，则称 $j(E)$为 E 的不变量。

Weierstrass 方程的射影平面表示式：令 $x=\dfrac{X}{Z}, y=\dfrac{Y}{Z}$

$$Y^2Z+a_1XYZ+a_3YZ^2 = x^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

$$F(X,Y,Z) = Y^2Z+a_1XYZ+a_3YZ^2-x^3-a_2X^2Z-a_4XZ^2-a_6Z^3$$

在 $P=(X,Y,Z)\in E$，$\dfrac{\partial F}{\partial X}, \dfrac{\partial F}{\partial Y}, \dfrac{\partial F}{\partial Z}$至少有一个非零，则称 Weierstrass 为非奇异。若 $\dfrac{\partial F}{\partial X}, \dfrac{\partial F}{\partial Y}, \dfrac{\partial F}{\partial Z}$在 P 点全为零，则称 P 点为奇异点，Weierstrass 称为奇异。

E 的 $j(E)=0$，则称 E 为超奇异。

8.6 $P+(Q+R)=(P+Q)+R$

$P+(Q+R)=(P+Q)+R$，若采用直接验证的方法，将不胜其烦，下面采用一种初等的证法。

椭圆曲线是一三次曲线，即满足 $F(x,y)=0$，$F(x,y)$的最高次方是 3，若 $F(x,y)$分解为一个一次方项，一是二次方项，则其图像为一圆锥曲线和一直线组成，若 $F(x,y)$分解为三个一次方项的乘积，则其图像是由三根直线组成的，因此两个三次曲线可能有相同部分，比如相同部分可能是一直线，也可能两个三次曲线共同部分为一圆锥曲线，两个椭圆可交于四点，两条椭圆曲线可交于 9 点，根据 Bezout 定理：两条代数和曲线 $F(x,y)=$

$0, G(x,y)=0$，它们依次为 m 和 n，且无共同部分，则两曲线的交点数为 mn 个，若交点数超过 mn，则有共同部分。

$m=3$ 时 $F=\sum_{\substack{i=0\\j=0\\i+j\leqslant 3}}^{3} a_{ij}x^iy^j$，共 10 项：$x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, c$。

$F(x,y)=0$ 和 $\lambda F(x,y)=0$ 表达同一曲线。

定理 8-2：两个三次多项式 $F_1(x,y)$、$F_2(x,y)$ 无公因式，则三次曲线 $F_1(x,y)=0, F_2(x,y)=0$，有 9 个交点，另有一个三次曲线 $F(x,y)=0$ 过两个三次曲线的 8 个交点，则必过第 9 个交点。

证　只要证 $F=c_1F_1+c_2F_2$ 即可，c_1、c_2 是任意实数，若 $F\neq c_1F_1+c_2F_2$，证其出现矛盾。

$F_1\neq cF_2$，否则 $F_1=0$ 和 $F_2=0$ 全同。

任给 A、B 两点，$F^*=F_{AB}=cF-c_1F_1-c_2F_2$，两个线性方程组解三个变量 c, c_1, c_2，使 $F^*=0$ 过 A, B 两点，F^* 的次方不超过 3，即 $\deg F^*\leqslant 3$，若 9 个交点 $P_1, P_2, \cdots, P_9$ 是三个三次曲线 $F_1=0, F_2=0, F^*$ 共过的点，F_{AB} 还过 A、B 两点。

$P_1, P_2, \cdots, P_8$ 最多有三点在一直线上，根据 Bezout 定理，一直线和一三次曲线只能交于三点，否则这条直线是 $F_1=0, F_2=0$ 两个三次曲线的共同部分，同样一二次曲线和一三次曲线将交于 6 点，所以 $P_1, P_2, \cdots, P_8$ 只有 6 点在一二次曲线上，若超过 6 点，则这二次曲线必是 $F_1=0$ 和 $F_2=0$ 的共同部分，与假设矛盾。

$P_1\sim P_8$ 中假定 P_1 和 P_2 在一直线 L 上，其余 $P_4, P_5, \cdots, P_8$ 在一圆锥曲线 C 上，必须考虑三种情况：

(1) P_3 在 L 上；

(2) P_3 在 C 上；

(3) P_3 既不在 L 上，也不在 C 上。

分别讨论如下：

(1) 此时，取 $A(\neq P_i, i=1,2,3)$ 为 L 上的一点，取 B 既不在 L 上，也不在 C 上，因 L 和 $F^*=0$ 有 4 点 P_1, P_2, P_3 和 A 共同，L 是 $F^*=0$ 的一共同部分，$F^*=0$ 的另一部分必须是 C，故 B 不能在 $F_{AB}=0$ 上导致矛盾。

(2) 这种情形取 $A(\neq P_j, j=3,4,\cdots,8)$ 在 C 上，B 既不在 L 上，也不在 C 上，则 $F^*=0$ 和 C 交多于 6 点，故 C 必然是共同部分，$F^*=0$ 的其他部分必然是 L，故与 $F^*=0$ 不能过 B 产生矛盾。

(3) 取 A 和 B 共在 L 上，可以证明 P_3 不在 $F_{AB}=0$ 上，导致矛盾。

最后导致 $F(x,y)=0$ 过 $F_1(x,y)=0, F_2(x,y)=0$ 的 9 个交点中的 8 点有 $F(x,y)=c_1F_1(x,y)+c_2F_2(x,y)=0$，必就过第 9 点，如图 8-5 所示。

现在来证明椭圆曲线上关于加法的结合律成立：

图 8-5 符号说明：

P_i 和 P_j 的连线交 E 于 P_iP_j，例如 P_1P_2 表示 P_1 点与 P_2 点连线交椭圆曲线的交点 $O(P_iP_j)=P_i+P_j$，其中 O 是无穷远点，表示 O 与 P_iP_j 连线与 E 的交点的连线交于 P_i+

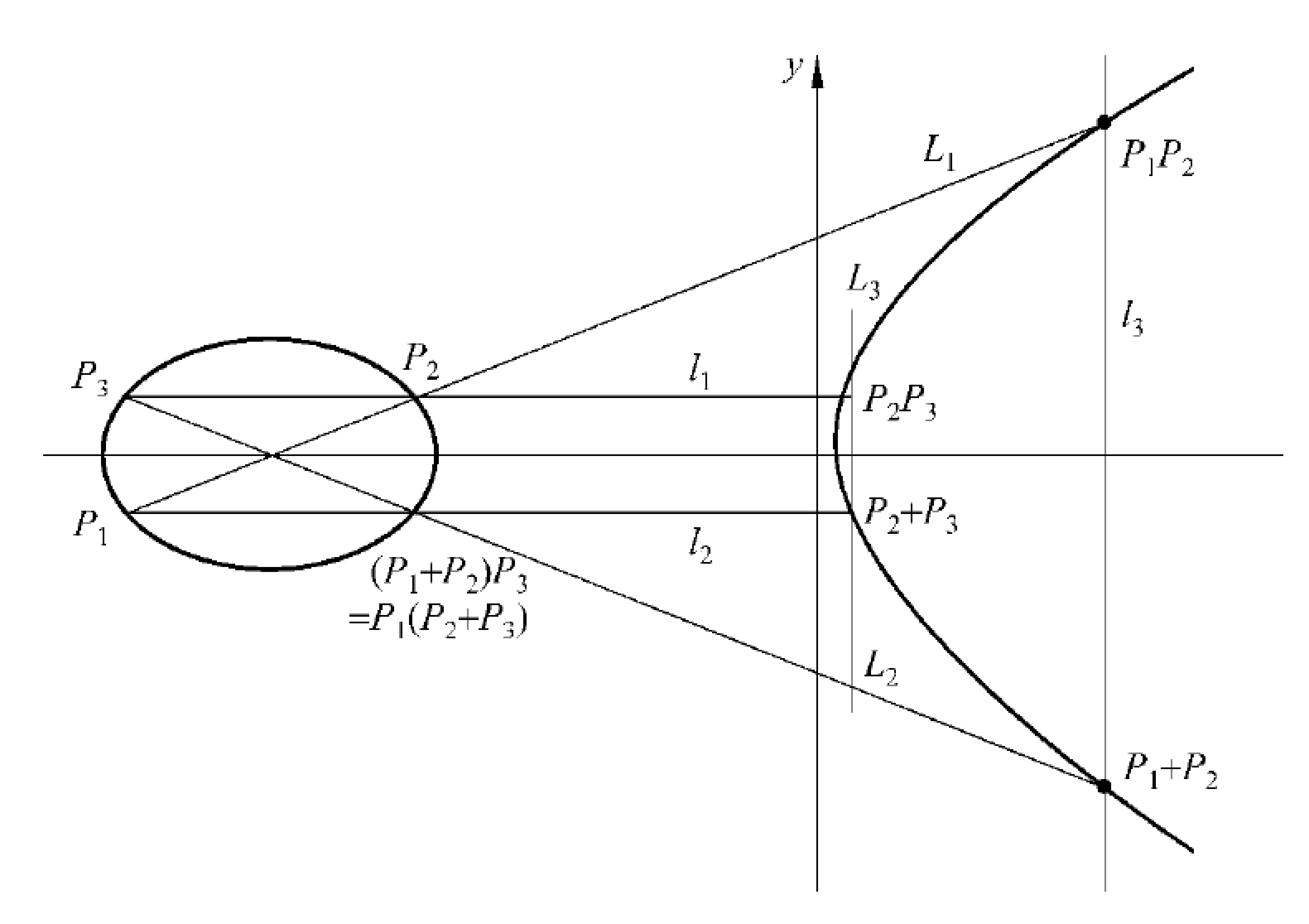


图 8-5　椭圆曲线

P_j,O 是 Abel 群的单位元。

有两组直线$\{l_i:i=1,2,3\}$和$\{L_j:j=1,2,3\}$分别组成由三条直线构成的三次曲线 C_1 和 C_2,l_i 和 L_j 的交点如下。

	L_1	L_2	L_3
l_1	P_2	P_3	P_2P_3
l_2	P_1	T	P_2+P_3
l_3	P_2P_3	P_1+P_2	O

T 表示 $P_1(P_2+P_3)=(P_1+P_2)P_3$。

E 通过 C_1 和 C_2 的 8 个公共点：$P_1,P_2,P_3,P_1+P_2,P_1P_2,P_2+P_3,P_2P_3,O$。

根据本节定理 $P_1(P_2+P_3)$和$(P_1+P_2)P_3$ 作为第 9 个公共点，

Hasse 定理：

$\#E(F_q)=q+1-t$。

$|t|=2\sqrt{q}$。

证　从略。

8.7　椭圆曲线的密码

(1) Diffie-Hellman 的密钥互换。

S1 通信双方公开选定素数 P 及 α,$2\leqslant\alpha\leqslant p-2$。

S2 A 随机选取 x,$1\leqslant x\leqslant p-2$,计算 $k_A\equiv\alpha^x\pmod p$,A 将 k_A 送 B;

　B 随机选取 y,$1\leqslant y\leqslant p-2$,计算 $k_B\equiv\alpha^y\pmod p$,B 将 k_B 送 A。

S3 A 收到 k_B 后计算 $k_{AB}\equiv(\alpha^y)^x\pmod p$;

　B 收到 k_A 后计算 $k_{AB}\equiv(\alpha^x)^y\pmod p$;

$(\alpha^x)^y(\bmod p)=(\alpha^y)^x(\bmod p)=\alpha^{xy}(\bmod p)$。

① * 椭圆曲线上的密钥互换协议：

S1 A,B 双方公开选定有限域 $GF(2^k)$上的椭圆曲线 E 及 $P\in E(GF(2^k))$。

S2 A 随机选取 x, $0\leqslant x\leqslant \# E$,计算 $k_A=xP$,并将 k_A 送给 B;

B 随机选取 y, $1\leqslant y\leqslant \# E$,计算 $k_B=yP$,并将 k_B 送 A。

S3 B 收到 k_A 后计算 $k_{AB}=yk_A=y(xP)$;

A 收到 k_B 后计算 $k_{AB}=xk_B=x(yP)$。

② Elgamal 公钥：

系统提供大素数 p 及 $GF(p)$上的本原元素 g,用户 A 可选择 $x_A\in[0,1,\cdots,p-1]$计算 $y_A\equiv g^{x_A}(\bmod p)$。$y_A$ 是公开的,x_A 保密,A 的公钥$(p,g,g^{x_A}(\bmod p))$,B 向 A 送去信息 m 的加密过程 $0\leqslant m\leqslant g-1$:

S1 B 取 A 的公钥$(p,g,g^{x_A}(\bmod p))$。

S2 随机选择整数 k, $1\leqslant k\leqslant p-2$。

S3 计算 $h\equiv g^k(\bmod p)$, $d=m\,(g^{x_A})^k(\bmod p)$。

S4 B 向 A 送去(h,d)。

A 解密过程：

S1 计算 $h^{p-1-x_A}(\bmod p)$。

S2 $h^{-x_A}d(\bmod p)\equiv m$。

因 $h^{p-1-x_A}(\bmod p)\equiv(h^{p-1})h^{-x_A}\equiv(g^k)^{p-1}(\bmod p)\equiv(g^{p-1})^k(\bmod p)\equiv h^{-x_A}d(\bmod p)$,
$h^{-x_A}d\equiv g^{-x_Ak}m\,(g^{x_A})^k(\bmod p)\equiv m$。

(2) * 椭圆曲线上的 Elgamal 公钥密码。

系统公开选取椭圆曲线 E 及其一点 α。

B 向 A 保密通信过程：

用户 A 随机选取 u, $0<u<\# E$,作为私钥,$\beta_u=u\alpha$ 作为公钥。

B 向 A 保密送信息 $m=(m_1,m_2)$过程：

S1 计算 $uva=v(\beta_u)=(x_k,y_k)$,v 是 B 的私钥,B 向 A 送去(β_v,x_km_1,y_km_2)。

S2 A 收到(β_v,x_km_1,y_km_2)后计算 $u\beta_v=uva=(x_k,y_k)$,从 x_km_1 乘以 x_k^{-1} 得 m_1,再从 y_km_2 得 m_2。

公用 E, $\alpha\in E$,见图 8-6。

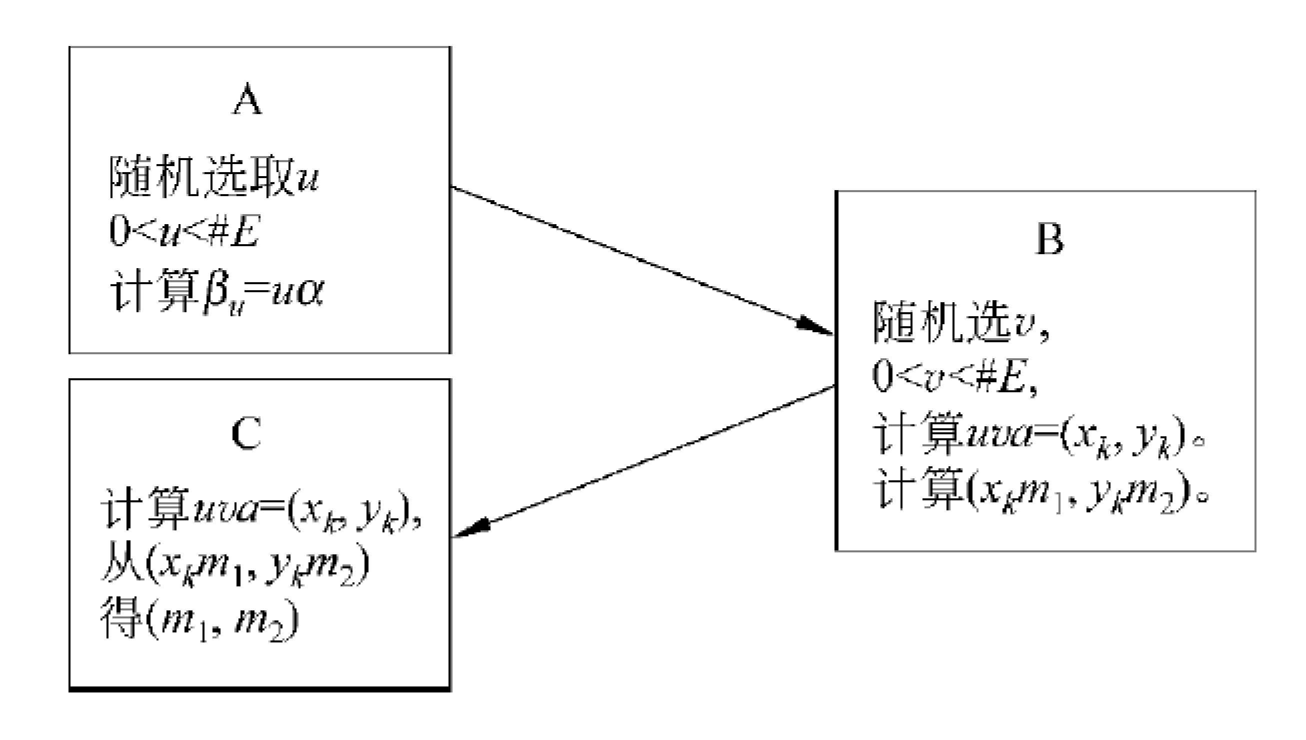


图 8-6 椭圆曲线上 Elgamal 公钥密码

8.8　若干算法

(1) 求 KP 的算法。

令 $K=(k_{r-1}k_{r-2}\cdots k_1k_0)_2$, $k_i\in\{0,1\}$, $0\leqslant i\leqslant r-1$, $k_{r-1}=1$,

$KP=\sum_{j=0}^{r-1}k_j2^jP=2(\cdots(2k_{r-1}P+k_{r-2}P)+\cdots)+k_0p$。

S1 $Q\leftarrow P$, $i\leftarrow r-1$。

S2 若 $i\geqslant 0$ 则转 S3,否则输出 Q,结束。

S3 $Q\leftarrow Q+Q$,

若 $k_l=1$,则作 $Q\leftarrow Q+P$, $i\leftarrow i-1$,转 S2。

(2) $K=(k_tk_{t-1}\cdots k_1k_0)_b$, $b=2^h$, $h\geqslant 1$,求 KP, $P\in E$。

S1 $P_0\leftarrow 0$, $i\leftarrow 1$。

S2 若 $i\leqslant 2^h-1$,则作

　始 $P_i\leftarrow P_{i-1}+P_i$, $i\leftarrow i+1$,转 S2 **终**。

S3 $Q\leftarrow 0$, $i\leftarrow t$。

S4 若 $i\geqslant 0$,则作

　始 $Q\leftarrow 2^hQ$, $Q\leftarrow Q+P$, $i\leftarrow i-1$ 转 S4 **终**。

S5 输出 Q。

(3) 已知 $P\in E$, $K=(k_tk_{t-1}\cdots k_1k_0)_b$, $b=2^h$, $h\geqslant 1$,求 KP。

若 $k_i\neq 0$,令 $k_i=2^{h_i}u_i$, u_i 是奇数;若 $k_i=0$,则 $h_i=0$, $u_i=0$。

S1 $P_i\leftarrow 0$, $P_1\leftarrow P$, $P_2\leftarrow 2P$, $i\leftarrow 1$。

S2 若 $i\leqslant 2^{h-1}-1$,则

　作**始** $P_{2i+1}\leftarrow P_{2i-1}+P_2$, $i\leftarrow i+1$ 转 S2 **终**。

S3 $Q\leftarrow 0$, $i\leftarrow t$。

S4 若 $i\geqslant 0$ 则作

　始 $Q\leftarrow 2^{h_i}(2^{h-h_i}Q+P_{u_i})$, $i\leftarrow i-1$,转 S4 **终**。

S5 输出 Q。

(4) $P\in E$, $K=(k_hk_{h-1}\cdots k_0)_2$, $h\geqslant 1$,求 KP。

S1 $P_1\leftarrow P$, $P_2\leftarrow 2P$, $i\leftarrow 1$。

S2 若 $i\leqslant 2^{h-1}-1$ 则作 $P_{2i+1}\leftarrow P_{2i-1}+P_2$。

S3 $Q\leftarrow 0$。

S4 $i\leftarrow h$。

S5 若 $i\geqslant 0$ 则转 S6,否则转 S8。

S6 $k_i=0$,则作

　始 $Q\leftarrow 2Q$, $i\leftarrow i-1$ **终** 否则转 S7。

S7 找最大的子串 $(k_ik_{i-1}\cdots k_l)$, $i-l+1\leqslant h$, $k_l=1$,

　$Q\leftarrow 2^{i-l+1}Q+P_{(k_i\cdots k_l)_2}$, $i\leftarrow l-1$,转 S5。

S8 输出 Q。

例 8-17 $K=(101\ 101\ 111\ 000\ 101)_2=11\ 749$，$h=3$，如表 8-1 所示。

表 8-1 KP 算法

i	Q	最长字符串
13	O	101
10	$5P$	101
7	$((5\times 8)+5)P=45P$	111
6	$((45\times 8)+7)P=367P$	
5	$(2\times 367)P=734P$	
2	$2\times 734P=1468P$	101
0	$((1468\times 8)+5)P=11\ 749P$	

8.9 复合域 $G((2^n)^m)$ 简介

在椭圆曲线的研究中引进了复合域：

$A(x)\in GF((2^n)^m)$：

$A(x)=a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0$。

$a_i\in GF(2^n)$。

(1) 关于 $GF(2^n)$ 的乘法，所有 $GF(2^n)$ 的非零元素都表示以本原元素 w 的次方，$k=\log(w^k)$，$w^k\in GF(2^n)$，$k\in\{1,2,\cdots,2^n-1\}$，$GF(2^n)=\{0,w,w^2,\cdots,w^{2n-1}=1\}$。

$w^k=\text{antilog}(k)=\text{antilog}(w^k)$，$w^k\in GF(2^k)$，$k\in\{1,2,\cdots,2^n-1\}$。

最后，两个 $GF(2^n)$ 的元素 w_i、w_j 的乘法可转换成整数的加法。

$w_iw_j=\text{antig}(\log(w_i)+\log(w_j))(\text{mod } 2^{n-1})$。

可通过预先计算好的表 log 和 antiglog 表。

(2) 关于 $GF((2^n)^m)$ 的加法：

$C(x)=A(x)+B(x)$，$A(x)$，$B(x)$，$C(x)\in GF((2^n)^m)$，

$=(c_{m-1}x^{m-1}+\cdots+c_1x+c_0)$

$=(a_{m-1}x^{m-1}+\cdots+a_1x+a_0)+(b_{m-1}x^{m-1}+\cdots+b_1x+b_0)$，

$c_i=a_i+b_i\in GF(2^n)$。

(3) $GF((2^n)^m)$ 的乘法：

$C(x)=A(x)\times B(x)\text{mod } P(x)$，

$P(x)$ 是 $GF((2^n)^m)$ 上不可化约的多项式。

在讨论 $GF((2^n)^m)$ 乘法之前，先介绍 Karatsuba-Ofman 算法。

从最原始的整数乘法来看，设 A、B 都是 n 位数，一般要作 n^2 次一位数的乘法，似乎这是天经地义的，其实不然。

若 $A=(a_110^{\frac{n}{2}}+a_2)$，$B=(b_110^{\frac{n}{2}}+b_2)$，这里 a_1，a_2，b_1，b_2 都是 2^{n-1} 位数。

$AB=(a_1+a_2)(b_1+b_2)+a_1b_1+a_2b_2$。

令 $p=(a_1+a_2)(b_1+b_2)$，$q=a_1b_1$，$r=a_2b_2$。

$AB=q\times 10^n+(p-q-r)10^{\frac{n}{2}}+r$。

这样只做 3 次 $\frac{n}{2}$ 位的乘法若只考虑一位数乘法的次数。

令 $N=2^n$。

$T_n=3T_{n-1}$，$T_0=1$，

$T_n=3^n$，$N=2^n$，$\log_2 N=n$。

$\log_2 T_n=n\log_2 3$，$T_n=2^{n\log_2 3}=N^{\log_2 3}$。

例 8-18　$A=2348$，$B=3825$。

$a_1=23$，$a_2=48$，$b_1=38$，$b_2=25$。

$p=(a_1+a_2)(b_1+b_2)=71\times 63=4473$。

$q=a_1b_1=874$，$r=a_2b_2=1200$。

$AB=8\,740\,000+(4473-874-1200)\times 100+1200=8\,740\,000+239\,900+1200=8\,981\,100$。

其中 $q\times 10^n$ 和 $(p-q-r)\times 10^{\frac{n}{2}}$，乘 10^n 和乘 $10^{\frac{n}{2}}$，只做移位运算。

对于次方为 2^l-1 的两个多项式之积，$GF((2^n)^m)$ 的两个多项式之积包含两个多项式之积和求模，其中最主要的运算在于求最高次方为 2^l-1，系数在 $GF(2^n)$ 的两个多项式 $A(x)$ 和 $B(x)$ 之积，如果直接求积，必须作 m^2 次在 $GF(2^n)$ 域上的元素相乘。

$C(x)=A(x)B(x)$，$\deg(C(x))\leqslant 2m-2$，若将 $A(x)$，$B(x)$ 分为前后两半：

$A(x)=x^{\frac{m}{2}}(a_{m-1}x^{\frac{m}{2}-1}+\cdots+a_{\frac{m}{2}})+(a_{\frac{m}{2}-1}x^{\frac{m}{2}-1}+\cdots+a_0)=A_nx^{\frac{m}{2}}+A_l$。

$B(x)=x^{\frac{m}{2}}(b_{m-1}x^{\frac{m}{2}-1}+\cdots+b_{\frac{m}{2}})+(b_{\frac{m}{2}-1}x^{\frac{m}{2}-1}+\cdots+b_0)=B_nx^{\frac{m}{2}}+B_l$。

利用 Karatsuba-Ofman 算法可得：乘法数 $=m^{\log_2 3}$，$O(n^{\log_2 3})$，可见并非一定要作 m^2 次一位数相乘。

(4) 求逆 A^{-1}：

$A\in GF((2^n)^m)$，$A\neq 0$。

$A(x)=a_{m-1}x^{m-1}+\cdots+a_1x+a_0$，$a_i\in GF(2^n)$，

利用 Fermat 定理：

$A^{2^{mn}-1}=AA^{2^{mn}-2}=1$，$\forall A\in GF((2^n)^m)\backslash\{0\}$。

$A^{-1}=A^{2^{mn}-2}$。

下面介绍 Paar 提供的方法：

$A^{-1}=(A^r)^{-1}A^{r-1}$，$r=(2^{mn}-1)/(2^n-1)$。

此时 $A^r\in GF(2^n)$。

S1 计算 A^{r-1}。

S2 计算 $AA^{r-1}=A^r$。

S3 求 $(A^r)^{-1}$。

S4 $(A^r)^{-1}A^{r-1}=A^{-1}$。

习　　题

$y^2=x^3+x+4, K=GF(23)$。

1. $P=(0,2)$，求 $2P,3P,4P$。
2. $P=(13,12)$，求 $2P,3P,4P$。
3. $P=(11,9)$，求 $2P,3P,4P$。
4. $P=(1,12)$，求 $2P,3P,4P$。
5. $P=(7,20)$，求 $2P,3P,4P$。
6. $P=(7,11)$，求 $2P,3P,4P$。
7. $P=(17,16)$，求 $2P,3P,4P$。
8. $P_1=(0,21), P_2=(0,2)$，求 P_1+P_2。

第 9 章　Lenstra 因数分解法

9.1　mod n 的椭圆曲线

定义 9-1：假定 p 是 n 的素因子，且 $p>3$，m 是任一整数，若 x_1, x_2 是任意两个有理数，其分母与 m 互素，但 x_1-x_2 化约到最后，分子被 m 除尽的分数时，写作 $x_1 \equiv x_2 \pmod m$，以上对两个有理数 x_1 和 x_2，给出 $x_1 \equiv x_2 \pmod m$ 是对过去同余式概念的拓展。

可以证明若 x_1 是一分母与 m 互素的有理数，则存在唯一的整数 x_2，$0 \leqslant x_2 \leqslant m-1$，使得

$x_1 \equiv x_2 \pmod m$。

若 $x_1 = \dfrac{a}{b}$，$(b,m)=1$。

则 $x_1 - x_2 = \dfrac{a-bx_2}{b}$，

$bx_2 \equiv a \pmod m$。

在 $(b,m)=1$ 的条件有唯一解 x_2，

$0 \leqslant x_2 \leqslant m-1$。

现在将上述的同余概念用于椭圆曲线 E：

定义 9-2：设 $P(x,y) \in E$，定义

$$P(\bmod m) \triangleq (x(\bmod m), y(\bmod m))$$

$P(\bmod m)$ 为 $E(\bmod m)$ 椭圆曲线上的点。

将第 8 章讨论的有关椭圆曲线的性质均可推广到 $E(\bmod m)$ 上来，但是它的每项都理解为 mod m，比如 $y^2=x^3+ax+b$，其中 a、b 都应理解为 $a(\bmod m)$、$b(\bmod m)$，分母 (x_1-x_2) 理解为 (x_1-x_2) 的逆。

$E(\bmod m)$ 上的无穷远点 $O(\bmod m)$ 表示椭圆曲线 E 上点的坐标，其分母含有 m 的因子的点。

定理 9-1：E：$y^2=x^3+ax+b$，$a,b \in Z$，$\gcd(4a^3+27b^2, n)=1$。

P_1, P_2 是 E 上两点，$P_1 \neq P_2$。它们的坐标的分母与 n 互素的充要条件是：不存在素数 $p \mid n$，使得曲线 $E(\bmod p)$ 上 $P_1(\bmod p)$ 和 $P_2(\bmod p)$ 之和为 $E(\bmod p)$ 的无穷远点 $O(\bmod p)$，其中 $E(\bmod p)$ 是 $GF(p)$ 域上的椭圆曲线，$O(\bmod p)$ 为 $GF(p)$ 域的椭圆曲线的无穷远点（即指的是 $(x,y) \in E$，其坐标的分母有 p 因子的点）。

说明一下，E：$y^2=x^3+ax+b$，$\mathrm{char}(V_1) \neq 2,3$，$\Delta=-16(4a^3+27b^2)$，$j=1728\dfrac{4a^2}{4a^3+27b^2}$，Weiestrass 定义的椭圆曲线是奇异的当且仅当 $\Delta=0$。

证　必要性，即已知 $P_1=(x_1,y_1)$，$P_2=(x_2,y_2)$，$P_1+P_2=(x_3,y_3)$，它们的坐标分母都和 n 互素，p 是 n 的素因子，则 $P_1(\mathrm{mod}\ p)+P_2(\mathrm{mod}\ p)\neq O(\mathrm{mod}\ p)$，分 $x_1\not\equiv x_2(\mathrm{mod}\ p)$ 和 $x_1\equiv x_2(\mathrm{mod}\ p)$ 两种情况：

(1) $x_1\not\equiv x_2(\mathrm{mod}\ p)$，即 $P_1\neq P_2$ 根据

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2,y_3=-y_1+\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)$$

显然 $P_1(\mathrm{mod}\ p)+P_2(\mathrm{mod}\ p)\neq O(\mathrm{mod}\ p)$ 成立。

(2) $x_1\equiv x_2(\mathrm{mod}\ p)$，又分 $P_1=P_2$ 和 $P_1\neq P_2$ 两种可能。

若 $P_1=P_2$，则 $P_1+P_2=2P_1$，这时

$$x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1,y_2=-y_1+\left(\frac{3x_1^2+a}{2y_1}\right)(x_3-x_1) \tag{B}$$

其分母 $2y_1$ 不被 p 除尽，如若不然必有 $P|(3x_1^2+a)$。这说明 x^3+ax+b 和它的导数有相同的零点 $x=x_1$，因 $4a^3-27b^2\not\equiv O(\mathrm{mod}\ p)$。

(注：请看本书第 8 章 8.2 节例。证明了 $f(x)=x^3+ax+b,y'=3x^2+a$ 有共同因子，则 $27b^2+4a^3=0$）这和 mod p 无重根的假设相矛盾。这就证明了 $P_1(\mathrm{mod}\ p)+P_2(\mathrm{mod}\ p)\neq O(\mathrm{mod}\ p)$。

最后假定 $x_2\equiv x_1(\mathrm{mod}\ p)$，但 $P_1\neq P_2$，且 $x_1\neq x_2$，令 $x_2=x_1+p^rx$，x 分母和分子均无 p 的因子，$r\geqslant 1$。根据 P_1+P_2 的坐标的分母不含 p 的因子的假设

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2,y_3=-y_1+\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3) \tag{A}$$

故 $y_2-y_1=p^ry$ 必然成立，这就证明了

$$y_2\equiv y_1(\mathrm{mod}\ p)\text{或}P_1(\mathrm{mod}\ p)=P_2(\mathrm{mod}\ p)$$

另一方面：

$$\begin{aligned}y_2^2&=(x_1+p^rx)^3+a(x_1+p^rx)+b=x_1^3+3x_1^2p^rx+3x_1p^{2r}x^2+p^{3r}x^3+ax_1+ap^rx+b\\&\equiv x_1^3+3p^rx_1^2x+a_1x+ap^rx+b(\mathrm{mod}\ p^{r+1})\\&=x^3+ax_1+b+p^rx(3x_1^2+a)(\mathrm{mod}\ p^{r+1})\\&=y_1^2+p^rx(3x^2+a)(\mathrm{mod}\ p^{r+1})\end{aligned}$$

由于 $P_1\neq P_2$，但 $x_1\equiv x_2(\mathrm{mod}\ p)$，$y_1\equiv y_2(\mathrm{mod}\ p)$，所以

$$P_1(\mathrm{mod}\ p)+P_2(\mathrm{mod}\ p)=2P_1(\mathrm{mod}\ p)$$

$2P_1(\mathrm{mod}\ p)$ 为 $O(\mathrm{mod}\ p)$ 的充要条件是 $y_1\equiv y_2\equiv O(\mathrm{mod}\ p)$，这便有：

$(y_2^2-y_1^2)=(y_2-y_1)(y_2+y_1)$ 的分子可被 p^{r+1} 除尽，导致

$$3x_1^2+a\equiv 0(\mathrm{mod}\ p)$$

这是不可能的，因 $x^3+ax+b(\mathrm{mod}\ p)$ 没有重根，这就证明了必要条件。

充分性的证明，假定 n 的所有素因子 p 有 $P_1(\mathrm{mod}\ p)-P_2(\mathrm{mod}\ p)\neq 0(\mathrm{mod}\ p)$。证明 P_1+P_2 点坐标分母与 n 互素，也就是它们坐标的分母不被 n 的任何因子 p 除尽。

(1) 若 $x_2\not\equiv x_1(\mathrm{mod}\ p)$，根据 $P(\mathrm{mod}\ m)\triangleq(x(\mathrm{mod}\ m),y(\mathrm{mod}\ m))$ 可知 x_3,y_3 的分母不被 p 除尽，这时定理自然成立。

(2) 若 $x_2\equiv x_1(\mathrm{mod}\ p)$，因 $y^2=x^3+ax+b$，故 $y_2\equiv y_1(\mathrm{mod}\ p)$，

但 $P_1 \pmod p + P_2 \pmod p \neq 0 \pmod p$，故

$$y_2 \equiv y_1 \not\equiv 0 \pmod p$$

在 $x_1 \equiv x_2 \pmod p$，$y_1 \equiv y_2 \pmod p$ 的前提下，有两种可能：$P_1 = P_2$ 或 $P_1 \neq P_2$。

若 $P_1 = P_2$，$P_1 + P_2 = 2P_2$，从公式(A)，这时分母不存在 p 的因子。

若 $P_1 \neq P_2$，令 $x_2 = x_1 + p^r x$，$r \geqslant 1$，x 的分母不含 p 的因子。

所以 $x_2 - x_1 = p^r x$，$\dfrac{y_2^2 - y_1^2}{x_2 - x_1} \equiv 3x_1^2 + a \pmod p$。

故 $y_1 + y_2 \equiv 2y_1 \pmod p$。

$\dfrac{y_2^2 - y_1^2}{(y_2 + y_1)(x_2 - x_1)} = \dfrac{y_2 - y_1}{x_2 - x_1}$ 的分母不存在 p 的因子，从公式(A)的分母不存在 p 的因子，也就是说 $P_1 + P_2$ 的坐标的分母不含 p 的因子。证毕。

定义 9-3：给定一合数 n，要找一素数 p，使 $p \mid n$，$1 < p < n$。

(1) 随机生成椭圆曲线 E：$y^2 = x^3 + ax + b$ 及 E 上一点 $P(x, y)$。

方法是先随机产生一点 $P(x, y)$ 及整数 a，$b = y^2 - x^3 - ax$，再检验 $4a^3 + 27b^2 = 0$？以保证 $x^3 + ax + b = 0$ 没有重根，若 $4a^3 + 27b^2 = 0$ 则改变 a 重复以上步骤。

(2) 给出界 B 和 C，计算

$$k = \prod_{p_i \leqslant B} p_i^{\alpha_i}, p_i^{\alpha_i} \leqslant C, \forall p_i \leqslant B$$

(3) 计算 $kP \pmod n$，根据公式(A)、(B)，x_3 和 y_3 的分母分别为 $x_2 - x_1$ 及 $2y_1$，求 $(x_2 - x_1)$ 和 $2y_1 \pmod n$ 的逆时若发生困难，正好说明分母含有 n 的某一因数，转而求它和 n 的最大公约数，依据本节的定理 9-1 可知 $P_1 + P_2$ 的坐标含有 n 的因数 p 的分母，当且仅当

$$P_1 \pmod p + P_2 \pmod p = 0 \pmod p, p \mid n$$

或归结出 Lenstra 算法：设 n 是合数：

S1 在 $1 \sim n$ 间随机选取 x_1，y_1，b。

S2 令 E：$y^2 = x^2 + bx + c$，

$$P = (x_1, y_1) \in E\text{，其中 } c = y_1^2 - x_1^3 - bx_1$$

S3 计算 $d = \gcd(4b^3 + 27a^2, n)$，若 $d = n$，则转 S1，重新选择 b，若 d 是 $1 \sim n$ 间的数，则它是 n 的因数。

S4 选择 k 是小素数的幂次的乘积，例如：

$$k = \operatorname{lcm}\{1, 2, \cdots, h\}$$

h 是一整数。

S5 计算 $kP = \left(\dfrac{a_k}{d_k^2}, \dfrac{b_k}{d_k^2}\right)$。

S6 计算 $g = \gcd(d_k, n)$，若 $1 < g < n$，则 g 是 n 的素因子。

若 $g = 1$，即 d_k 和 n 互素，则转 S4 提高 k，也可以转 S1 选择新的椭圆曲线。若 $g = n$，则转 S4，降低 k。

在计算 kP 的过程中存在一个 k_1，使得 $k_1 P \pmod p = O \pmod p$，也就是 k_1 为 $P \pmod p$ 点阶的倍数，在计算过程中求 mod n 某分母的逆时，代以求 n 和分母的最大公

因数。这个最大公因数除非就是 n 本身，一般来说是 n 的因数，所以在计算 $kP(\mathrm{mod}\ n)$ 时，对某一 $p|n$，k 是 $P(\mathrm{mod}\ n)$ 的阶时，收获得一个 n 的公因子。

算法所选的 E 和 P 不成功时，换一组重新开始，但连续多次都失败的概率不大。

算法中涉及选两个整数 B 和 C，B 和 C 越大，使得找 $kP(\mathrm{mod}\ p)=0(\mathrm{mod}\ p)$ 的概率增加，然而计算时间也越长。

例 9-1　$n=5429$，试利用椭圆曲线对 n 进行因数分解。

设 $B=3$，$C=92$，E：$y^2=x^3+2x-2$，$P=(1,1)$，$2P=(\xi_1,\eta_1)$。

过 P 点的切线方程 $y=mx+b$：

$$m=\left.\frac{3x^2+2}{2y}\right|_{(1,1)}=\frac{5}{2},b=1-\frac{5}{2}=-\frac{3}{2}$$

$$y=\frac{5}{2}x+\left(1-\frac{5}{2}\right)=\frac{5}{2}x-\frac{3}{2}$$

$$\left(\frac{5}{2}x-\frac{3}{2}\right)^2=x^3+2x-\frac{3}{2}$$

$$2+\xi_1=\left(\frac{5}{2}\right)^2,\xi_1=\left(\frac{5}{2}\right)^2-2=\frac{17}{4}$$

$$\eta_1-y|_{x=\xi_1}=\frac{5}{2}\times\frac{17}{4}-\frac{3}{2}=\frac{85}{8}-\frac{3}{2}=\frac{85-12}{8}=\frac{73}{8}$$

$$2P=\left(\frac{17}{4},-\frac{73}{8}\right)$$

令 $\frac{17}{4}\equiv u(\mathrm{mod}\ 5429)$，$4u\equiv17(\mathrm{mod}\ 5429)$。

$u\equiv4076(\mathrm{mod}\ 5429)$。

$-\frac{73}{8}\equiv v(\mathrm{mod}\ 5429)$，$8v\equiv-73(\mathrm{mod}\ 5429)$，$v\equiv23\,843(\mathrm{mod}\ 5429)$。

当然也可以以下面步骤计算 $2P(\mathrm{mod}\ 5429)$

$$u\equiv\left(\frac{3+2}{2}\right)^2-2=\left(\frac{5}{2}\right)^2-2(\mathrm{mod}\ 5429)$$

$\frac{1}{2}$ 理解为 $2^{-1}(\mathrm{mod}\ 5429)$，$2^{-1}(\mathrm{mod}\ 5429)\equiv2715$，

$u\equiv(2715\times5)^2-2=(2717)^2-2\equiv4078(\mathrm{mod}\ 5429)$，

$v=-1+\left(\frac{5}{2}\right)\times\left(\frac{-13}{4}\right)=-1+(2715\times5)\times(-13\times4072)$

$=-1+(2717)\times(1354)\times(\mathrm{mod}\ 5429)=3884(\mathrm{mod}\ 5429)$，

$4^{-1}(\mathrm{mod}\ 5429)=4072$。

$5429=1357\times4+1$，

$1=5429-1357\times4$，

$4^{-1}\equiv-1357\equiv4072$。

类似可计算 $4P(\mathrm{mod}\ 5429)$，令 $2^2P(\mathrm{mod}\ 5429)=(u_2,v_2)$，

$$u_2=\left(\frac{3\times4076+2}{6788}\right)^2-8152(\mathrm{mod}\ 5429)$$

$$= \left(\frac{1349+2}{1339}\right)^2 - 2723 \pmod{5429}$$

$1339^{-1} \equiv 2826 \pmod{5429}$。

$$u_2 = (1551 \times 2826)^2 - 2723 \pmod{5429}$$
$$\equiv (1923)^2 - 2723 \pmod{5429} \equiv 780 - 2723 \pmod{5429}$$
$$\equiv -1943 \pmod{5429} \equiv 3486 \pmod{5429}$$
$$v_2 \equiv -3384 + (1551 \times 2826) \times (4076 - 3486) - 2723 \pmod{5429}$$
$$\equiv -3384 + 1923 \times 590 \pmod{5429}$$
$$\equiv -3384 + 5338 \pmod{5429}$$
$$\equiv 1954 \pmod{5429}$$

$4P \pmod{5429} = (3486, 1954)$。

用类似步骤计算 $2^{\alpha}3^{\beta}P \pmod{5429}$。

当 $\alpha=6, \beta=2$ 时发现分母与 5429 有公因数 61，$5429=61\times 89$。

例 9-2 $n=1\,715\,761\,513$。

$2^{1\,715\,761\,512} \equiv 93\,082\,891 \bmod 1\,715\,761\,513$，

根据 Fermat 定理，$2^{n-1} \not\equiv 1 \bmod n$，可见不是素数。

$\sqrt{1\,715\,761\,513} \approx 42\,422$ 可知 n 有小于 42 422 的素数因子 p。

选 E：$y^2 = x^3 + x - 9$，$P=(2,1)\in E$。

令 k 为

$$\operatorname{lcm}\{1,2,3,\cdots,117\} = 12\,252\,240$$

$k = 12\,252\,240 = (101\,110\,101\,111\,110\,001\,010\,000)_2$

$\quad = 2^4 + 2^6 + 2^{10} + 2^{12} + 2^{13} + 2^{14} + 2^{15} + 2^{17} + 2^{19} + 2^{20} + 2^{21} + 2^{23}$。

计算 $kP \pmod n$

$P=(2,1)$，

$2y\dfrac{dy}{dx} = 3x^2+1$，$\dfrac{dy}{dx} = \dfrac{3x^2+1}{2y}\Big|_{(2,1)} = \dfrac{13}{2}$，

过(2,1)点即线

$y-1 = \dfrac{13}{2}(x-2)$，$y = \dfrac{13}{2}(x-2)+1$，

$y^2 = \left(\dfrac{13}{2}x - \dfrac{11}{2}\right)^2 = x^3 + x - 9$，

$x^3 - \dfrac{169}{4}x^2 + \left(\dfrac{143}{2}+1\right) - \left(9 + \dfrac{121}{4}\right) = 0$。

但 $1 = 1\,715\,761\,513 - 4(428\,940\,378)$。

$4(-428\,940\,378) \equiv 1 \pmod n$，

$4^{-1} \equiv -428\,940\,378 \equiv 1\,286\,821\,135 \pmod{1\,715\,761\,513}$。

同理 $2^{-1} \equiv 857\,880\,756 \equiv 85\,788\,075 \pmod{1\,715\,761\,513}$。

过(2,1)点的切线交 E 于(ξ,η)点：

$$2.5 + \xi = 1\,286\,821\,135 \times 169, \xi = 217\,472\,771\,815 - 4$$

$\xi = 217\ 472\ 771\ 811 \equiv 1\ 286\ 821\ 173 \bmod (1\ 715\ 761\ 513)$

$\eta = 1\ 672\ 350\ 709$

$2P = (12\ 866\ 821\ 173, 1\ 672\ 350\ 709)$

同理可得

$2^2P = (1\ 334\ 478\ 523, 112\ 522\ 703)$

$2^3P = (9\ 127\ 789\ 305, 77\ 695\ 868)$

$2^4P = (385\ 062\ 894, 618\ 628\ 731)$

$2^5P = (866\ 358\ 838, 450\ 284\ 374)$

$2^6P = (904\ 716\ 938, 169\ 383\ 608)$

$2^7P = (808\ 694\ 477, 1\ 201\ 030\ 016)$

$2^8P = (572\ 301\ 268, 107\ 111\ 567)$

$2^9P = (1\ 512\ 647\ 092, 1\ 695\ 275\ 444)$

$2^{10}P = (1\ 858\ 186, 1\ 224\ 662\ 922)$

$2^{11}P = (1\ 550\ 404\ 618, 825\ 515\ 387)$

$2^{12}P = (1\ 519\ 325\ 194, 16\ 574\ 978\ 846)$

$2^{13}P = (522\ 917\ 322, 524\ 407\ 354)$

$2^{14}P = (25\ 207\ 285, 1\ 375\ 034\ 461)$

$2^{15}P = (781\ 360\ 494, 1\ 457\ 273\ 929)$

$2^{16}P = (1\ 108\ 412\ 304, 25\ 813\ 532)$

$2^{17}P = (435\ 914\ 774, 323\ 718\ 902)$

$2^{18}P = (1\ 399\ 483\ 199, 1\ 203\ 811\ 423)$

$2^{19}P = (778\ 823\ 593, 192\ 206\ 539)$

$2^{20}P = (853\ 199\ 887, 1\ 012\ 680\ 972)$

$2^{21}P = (501\ 929\ 966, 910\ 060\ 788)$

$2^{22}P = (1\ 315\ 182\ 921, 305\ 331\ 854)$

$2^{23}P = (257\ 200\ 250, 318\ 342\ 966)$

$2^{24}P = (385\ 062\ 894, 618\ 628\ 731)$

$2^4P + 2^6P = 16P + 64P = 80P$

过(385 062 894,618 628 731)和(904 716 938,1 693 830)引直线 $y = mx + b$,

$$m = \frac{618\ 628\ 731 - 169\ 383\ 608}{385\ 062\ 894 - 904\ 716\ 938} = -\frac{449\ 245\ 123}{519\ 654\ 044}$$

$$b = y - mx = 618\ 628\ 731 - \frac{449\ 245\ 123}{519\ 654\ 044} \times 385\ 062\ 894$$

$$= 618\ 628\ 731 - \frac{172\ 987\ 627\ 177\ 765\ 962}{519\ 654\ 044}$$

$$172\ 987\ 627\ 177\ 765\ 962 \equiv 884\ 611\ 387 (\bmod\ 1\ 715\ 761\ 513)$$

所以 $b = 618\ 628\ 731 - \dfrac{884\ 611\ 387}{519\ 654\ 044}$。

但 $\gcd(884\ 611\ 387, 519\ 654\ 044) = 1$,令

$$\frac{884\ 611\ 387}{519\ 654\ 044}=n$$

求 $519\ 654\ 044^{-1}(\bmod n)$。

$$n=519\ 654\ 044^{-1}\times 884\ 611\ 387$$

$$b=618\ 628\ 731-n$$

若 $y=mx+b$ 交 E 于(α,β)，则

$$\alpha+385\ 062\ 894+9\ 047\ 169+38\equiv 3m^2b$$

$$S_2=(2^4+2^6)P=80P=(\alpha,-\beta)$$

$$S_2=(2^4+2^6)P=80P=(831\ 572\ 269,1\ 524\ 749\ 603)$$

计算过程从略。

$$S_3=S_2+2^{10}P=1104P=(1\ 372\ 980\ 126,1\ 361\ 189\ 875)$$

$$S_4=S_3+2^{12}P=5200P=(303\ 639\ 172,374\ 618\ 943)$$

$$S_5=S_4+2^{13}P=13\ 392P=(243\ 887\ 465,4\ 582\ 074)$$

$$S_6=S_5+2^{14}P=29\ 776P=(317\ 266\ 292,18\ 428\ 261)$$

$$S_7=S_6+2^{15}P=62\ 544P=(425\ 351\ 528,95\ 871\ 325)$$

$$S_8=S_7+2^{16}P=193\ 616P=(845\ 805\ 016,877\ 478\ 209)$$

$$S_9=S_8+2^{19}P=717\ 904P=(1\ 070\ 680\ 397,744\ 910\ 034)$$

$$S_{10}=S_9+2^{20}P=1\ 766\ 480P=(543\ 241\ 897,1\ 394\ 639\ 550)$$

$$S_{11}=S_{10}+2^{21}P=3\ 863\ 632P=(331\ 651\ 823,1\ 280\ 931\ 959)$$

$$S_{12}=S_{11}+2^{23}P=12\ 252\ 240P=(421\ 401\ 044,664\ 333\ 727)$$

$$kP=12\ 252\ 240P=(421\ 401\ 044,664\ 333\ 727)(\bmod 1\ 715\ 761\ 513)$$

设对 n 的素因子提供任何信息，$b=3,4,\cdots,253$ 都未有任何结果：

$b=254$ 时，E：$y^2=x^3+254x-515$

$$(2^4+2^6+2^{10}+\cdots+2^{20}+2^{21})P=3\ 863\ 632P$$

$$=(390\ 104\ 967,128\ 395\ 638)(\bmod n)$$

$$2^{23}P=(520\ 835\ 552,974\ 225\ 979)(\bmod n)$$

为了求得 kP，必须求$(390\ 104\ 967,128\ 395\ 638)$和$(520\ 835\ 552,974\ 225\ 979)$的连线和 E 的交点，

$390\ 104\ 967-520\ 835\ 552=-130\ 730\ 585\equiv 1\ 585\ 030\ 928(\bmod n)$，

$\gcd(1\ 585\ 030\ 928,1\ 715\ 761\ 513)=26\ 927$，

$n=1\ 715\ 761\ 513)=26\ 927\times 63\ 719$，

$1\ 585\ 030\ 928=26\ 927\times 58\ 864$。

9.2　算法的补充

椭圆曲线分解因数法，根据在 $E,E_{a,b},a,b\in E_{a,b}$ 上点的加法构成 Abel 群，如何搜索群的元素使有利于问题的解决，技巧还有一些，现举例补充如下。

例 $n=44\ 023$，随机选 a,b，

$y^2 = x^3 + ax + b \pmod n$

取 $a = 13, X = (x, y) = (23\,482, 9274)$，

$b = y^2 - x^3 - ax \pmod n = 21\,375$。

计算 $X_i = i!\ X = (x_i, y_i), i = 1, 2, \cdots$直到 $X_i \pmod p$是 0。

$X_1 = X, X_2 = 2X_1$，

$m = \dfrac{3x_1^2 + a}{2y_1} \pmod n = 31\,095$，

$x_2 = m^2 - 2x_1 \pmod n \equiv 18\,935, y_2 = m(x_1 - x_2) - y_1 \pmod n \equiv 21\,838$，

$X_3 = 3 \cdot X_2 = (2 \cdot X_2) + X_2$，先计算 $2X_2$。

$m = \dfrac{3x_2 + a}{2y_2} \pmod n = 41\,645$，

令 $2X_2 = (x, y)$，

$x = m^2 - 2x_2 \pmod n = 26\,093, y = m(x_2 - x) - y_2 \pmod n = 7008$，

$(x, y) + X_2$，

$m = \dfrac{y_2 - y}{x_2 - x} \pmod n = 5816$，

$x_3 = m^2 - x - x_2 \pmod n = 15\,187$，

$y_3 = m(x - x_3) - y \pmod n = 29\,168$，

已有结果：

$i = 1 \quad X_1 = (23\,482, 9274)$，

$i = 2 \quad X_2 = (18\,935, 21\,838)$，

$i = 3 \quad X_3 = (15\,187, 29\,168)$，

$i = 4 \quad X_4 = (10\,532, 5412)$，

$X_5 = 5 \cdot X_4 = (2(2X_4)) + X_4$，

$2X_4 = (30\,373, 40\,140)$，

$2(2X_4) = (27\,556, 42\,335)$。

计算 $2(2X_4) + X_4$。

$m = \dfrac{42\,335 - 5412}{27\,556 - 10\,532} \pmod n$，

但 $27\,556 - 10\,532 = 17\,024$，mod n 不存在逆，

$\gcd(17\,024, n) = 133$。

$n = 133 \times 331$。

平方筛法举例：

令 $n = 327\,773, m = 726$。

n 的平方根附近的素数：

2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，

但 n 是平方剩余，mod：

3，7，11，13，17，41，53，61，67，

$B = \{-1, 2, 3, 7, 11, 13, 17, 41, 53, 61, 67\}$，

令 $A=X+m$，

$X=\{0,+1,-1,+2,-2,\cdots\}$，

$m^2-n=527\,076-527\,773=-697=-1\times17\times41$，

$(m+1)^2-n=2^2\times3^3\times7$，

$(m-1)^2-n=-1\times2^2\times3\times179$，

$(m+2)^2-n=-1\times3\times11\times109$，

…

$(m+7)^2-n=2^2\times3\times13\times61$，

$(m-7)^2-n=-1\times2^2\times3\times17\times53$，

…

$(m+20)^2-n=3\times11\times13\times67$，

$(m+24)^2-n=7\times11^2\times41$，

$(m-24)^2-n=-1\times11^2\times17^2$，结果见表 9-1。

表 9-1　Lenstra 1

X	$m+x$	$(m+x)^2-n$	因　子	向　量
0	726	−697	$-1\times17\times41$	(1,0,0,0,0,0,1,1,0,0,0)
1	727	756	$2^2\times3^3\times7$	(0,2,3,1,0,0,0,0,0,0,0)
2	728	2211	$3\times11\times67$	(0,0,1,0,1,0,0,0,0,0,1)
5	731	6588	$2^2\times3^3\times61$	(0,2,3,0,0,0,0,0,0,1,0)
7	733	9516	$2^2\times3\times13\times61$	(0,2,1,0,0,1,0,0,0,1,0)
−7	719	−10 812	$-1\times2^2\times3\times17\times53$	(1,2,1,0,0,0,1,0,1,0,0)
10	736	13 923	$3^2\times7\times13\times17$	(0,0,2,1,0,1,1,0,0,0,0)
−13	713	−19 404	$-1\times2^2\times3^2\times7^2\times11$	(1,2,2,2,1,0,0,0,0,0,0)
17	743	24 276	$2^2\times3\times7\times17^2$	(0,2,1,1,0,0,2,0,0,0,0)
−17	709	−25 092	$-1\times2^2\times3^2\times17\times41$	(1,2,2,0,0,0,1,1,0,0,0)
20	748	28 743	$3\times11\times13\times67$	(0,0,1,0,1,1,0,0,0,0,1)
24	750	34 727	$7\times11^2\times41$	(0,0,0,1,2,0,0,1,0,0,0)
−24	702	−34 969	$-1\times11^2\times17^2$	(1,0,0,0,2,0,2,0,0,0,0)

$X=1$ 和 $X=17$ 有：

$727^2\times743^2\equiv3^2\times17^{-2}\pmod n$，

$727^2\times743^2\times\pmod n\equiv223\,754$，

$3\times17^{-1}\bmod n=186\,273$，

$527\,773=31\,045\times17+8$，

$17=2\times8+1$，

$1=17-2\times8=17-2\times(527\,773-31\,045\times17)=61\,091\times17-2n$，

$17^{-1} \pmod n \equiv 62\,091$，

$727 \times 743^{-1} \times \pmod n = 223\,754$，

$3 \times 17^{-1} \pmod n \equiv 186\,273$，

$223\,754 - 186\,273 = 37\,481$，

$\gcd(37\,481, n) = 1013$，

所以 $527\,773 = 1013 \times 521$。

习　题

1. $n = 82\,123$，试用 Lenstra 算法分解因数。
2. $2^{32} + 1$ 试用两种方法因数分解。
3. $2^{64} + 1$ 试用不同方法因数分解。

第 10 章　信息论及编码

10.1　导　　论

前面讨论的内容基本上是与密码有关的数学问题，通信保密用密码是为了信息的安全。现在继续讨论另一类的信息安全问题。例如卫星远距离的图像传输，计算机系统的数据传送都是通过信道。难免会受到随机的噪声干扰，使之发生错误，这就需要通过另一类的编码使之能纠正错误，密码是编码，纠错码也是一种编码。

不是特别声明，都假定信息流通都是 0，1 符号串流，信道受到随机干扰使 0 变 1，1 变 0，而且 0 变 1 和 1 变 0 的概率是一样的，这样的信道称为二元对称信道，如图 10-1 所示 0 变 1，1 变 0 的概率相同为 p，不改变的概率则是 $1-p$。

图 10-1　0↔1 变化相同图

最简单的办法是重发，比如重复发送信息 3 遍或 5 遍，收信方收到的三次或五次信道，相同的位则认为是真的，不同的位总有一个占多数，则采取“少数服从多数的原则”来决定处理。举个例子传输一个 0，重复三遍是 000，若出一个错可能是 001，010，100，收到的三次有两次是 000，一次为 010，则按 0 处理，根据是出两次错的概率为 $p^2<p$。

例 10-1　二元对称信道，出错的概率 $p=0.001$，若采用重播三次的方案，求传输出错的概率。

一个字符传三次出两个错的概率是

$$\binom{3}{2}\times 0.001^2\times(1-0.001)=3\times\left(\frac{1}{10}\right)^6\times 0.999=2.997\times\frac{1}{10^6}<0.000\ 003$$

本来传三次均出错的概率是 $(0.001)^3=\frac{1}{10^9}$，因此连传三遍而仍然是错传的概率下降到不足 0.000 003。

10.2　Hamming 距离

n 维 0.1 向量 $X=(x_1,x_2,\cdots,x_n)$，$x_i\in\{0,1\}$，$i=1,2,\cdots,n$，其中非零元素个数用 $w(X)$ 表示它，称为 X 的权，例如 $X=0010101$，则 $w(X)=3$。

定义 10-1：两个 n 维 0.1 向量 $X=(x_1,x_2,\cdots,x_n)$，$Y=(y_1,y_2,\cdots,y_n)$，

令 $d(X,Y)=w(X\oplus Y)=(x_1\oplus y_1)+(x_2\oplus y_2)+\cdots+(x_n\oplus y_n)$

其中$\oplus$是 mod 2 的加，$0\oplus 0=0$，$1\oplus 0=0\oplus 1=1$，$1\oplus 1=0$，

例如 $X=(010100)$，$Y=(110010)$，

$d(X,Y)=w(100110)=3$，

X 和 Y 的 Hamming 距离有如下几个性质：

(1) $d(X,Y)=0$，则 $X=Y$。

(2) $d(X,Y)=d(Y,X)$。

(3) $d(X,Y)\leqslant d(X,Z)+d(Z,Y)$。

(1)和(2)两个性质是显而易见的，性质(3)即三角形的两边之和大于等于第三边，这里讲的是 Hamming 距离，所以还得加以证明，设 $X=(x_1,x_2,\cdots,x_n)$，$Y=(y_1,y_2,\cdots,y_n)$，$Z=(z_1,z_2,\cdots,z_n)$，若 $x_i\neq z_i$，$y_i\neq z_i$，则 $x_i\neq y_i$，明白这个道理，性质(3)便不难理解了。

10.3　码　　字

编码的传输过程如图 10-2 所示。

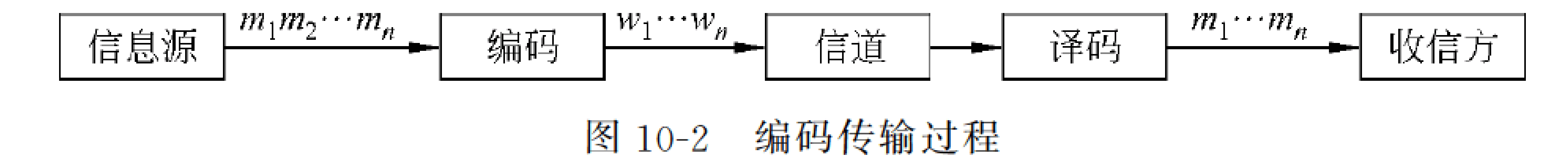


图 10-2　编码传输过程

比如 3 位的信息字对应一 6 位的码字的编码 C 如表 10-1 所示。

表 10-1　编码 C

信　息　字	码　　字	信　息　字	码　　字
000	000000	100	100011
001	001110	101	101101
010	010101	110	110110
011	011011	111	111000

000 信息字，若编码后正确传送应是 000000，若出错为 001000，码字上没有这码字，便知道是出错了，不是码的字就称为字，两个码字之间都存在有距离，其中最小的用 $d_{\min}$ 表示，即 $d_{\min}=\min\limits_{c_i,c_j\in C}\{d(c_i,c_j)\}$。

表 10-2 就是前一例子的两两码字的 Hamming 距离表。

表 10-2　(X,Y)对应表

Y \ X	000000	001110	010101	011011	100011	101101	110110	111000
000000	—	3	3	4	3	4	4	3
001110	3	—	4	3	4	3	3	4
010101	3	4	—	3	4	3	3	4

续表

X / Y	000000	001110	010101	011011	100011	101101	110110	111000
011011	4	3	3	—	3	4	4	4
100011	3	4	4	3	—	3	3	4
101101	4	3	3	4	3	—	4	3
110110	4	3	3	4	3	4	—	3
111000	3	4	4	4	4	3	3	—

定理 10-1：编码 C 当它的 $d_{\min}=d$ 时能检出 $d-1$ 位或小于 $d-1$ 位的错。

证　所谓能检出 $d-1$ 位错误是指码字在传输过程中出现了 $d-1$ 位错误能被发现，并提出来，之所以能被发现，因出错后的字不是码字。如果出错后变为另一个码字，则识别不了检查出有错，又不能断定正确的应是什么，只能诉之请求重发。

因为编码 C 的最短距离是 d，任何一码字受到小于或等于 $d-1$ 位的干扰不可能错误到使之成为另一码字，是字而不是码字，所以错误能被检查出来，如果某个码字传输出错达到 d 位，有可能被识别为别的码字，错误则无法查出来。

定理 10-2：编码 C 的 $d_{\min}=2t+1$，则能纠正 t 位的错误。

证　设 E 是被传输的码字，按收到是字 R，$d(Z,R)\leqslant t$，则不存在码字 Y，使 $d=(Y,R)\leqslant t$，否则

$$d(Z,Y)\leqslant d(Z,R)+d(R,Y)\leqslant t+t=2t<2t+1$$

与定理的假设 $d_{\min}=2t+1$ 相矛盾。

译码的原则“最大似然”准则，R 跟哪个码字（比如 Y）的 Hamming 距离最近，就译成码字 Y 传输出去。

10.4　熵 的 概 念

随机事件的特点是它的不确定性，它的出现的概率是对它不确定性的一种度量，概率越小其不确定性越大，概率等于 1 为确定性事件，即必然事件，概率为 0 为不可能事件。

信息论首先要解决对信息量的度量，直觉上对不确定事件其不确定性越大的信息越关注，确定性事件被看作毫无信息量或信息量等于零。比如听有人说“太阳从东方升起”，你会觉得那是一句废话，它没有任何新信息，如若有人发现“天空出现不明飞行物”，将无疑会引起许多人的好奇心而争相一睹。

从直观上看 k 个等概率事件将随 k 的增大，其不确定性随之增大，$k=1$ 时为确定性事件，不确定性度量结果是 k 的函数，设为 $f(k)$，$f(1)=0$，若 $k_1<k_2$，则 $f(k_1)<f(k_2)$。

若事件 A 有 h 个等概率事件，B 为有 k 个等概率事件，则 A 与 B，即 $A\cap B$ 有 hk 个等概率事件，它的不确定性超过 A 或 B，即 $f(hk)>f(h)$，$f(hk)>f(k)$。

根据上述特点，不妨令 $f(hk)=f(h)+f(k)$ 或 $f(k)=\log k=-\log\dfrac{1}{k}$。

以后不特别说明对数都以 2 为底，即这里“单位”为一个比特位，也就是两个等概率的事件，其不确定性为一个单位：比特。

当然 log 也可以以 e 为底，其单位是 nat，换底公式：$\log_a x=\dfrac{\log_b x}{\log_b a}$，1nat＝1.44 比特。

还可将上面的概念进一步拓展，设事件 $A=\{A_1,A_2,\cdots,A_n\}$，其中 A_i 出现的概率为 p_i，$i=1,2,\cdots,n$，$p_1+p_2+\cdots+p_n=1$。定义 $I(A_i)=-\log p_i$ 作为对 A_i 的信息量的度量，令 $H(A)=-p_1\log p_1-p_2\log p_2-\cdots-p_n\log p_n$。作为事件 A 的熵，用来度量 A 的不确定性，$H(A)$越大，表示 A 的不确定性也越大，而且可见 $H(A)$实际上是各事件 A_i 的信息量 $H(A_i)$的平均值，或数字期望值。

例 10-2 有一箱里装 20 个球，其中白球 10 个，红球 5 个，黑球 5 个，从箱中任取一球作为事件 A，取出白球，红球，黑球的概率依次为 $p_1=\dfrac{1}{2}$，$p_2=p_3=\dfrac{1}{4}$。

则 $H(A)=-\dfrac{1}{2}\log\dfrac{1}{2}-\dfrac{1}{4}\log\dfrac{1}{4}-\dfrac{1}{4}\log\dfrac{1}{4}=\dfrac{1}{2}\log 2+\dfrac{1}{2}\log 4=1.5$ 比特。

例 10-3 掷一骰子有 6 种状态，而且机会均等，作为事件 A，则 $H(A)=\log 6=2.5850$比特。

掷两个骰子有 36 状态，作为 A：和为 2 的有 1 种，和为 3 的有 2 种，和为 4 的有 3 种，和为 5 的有 4 种，和为 6 的有 5 种，和为 7 的有 6 种，和为 8 的有 5 种，和为 0 的有 4 种，和为 10 的有 3 种，和为 11 的有 2 种，和为 12 的有 1 种。

$$
\begin{aligned}
H(A)&=-\frac{2}{36}\times\log\frac{1}{36}-\frac{4}{36}\times\log\frac{2}{36}-\frac{6}{36}\times\log\frac{3}{36}-\frac{8}{36}\times\log\frac{4}{36}\\
&=\frac{-2}{36}\times\log\frac{1}{36}-\frac{4}{36}\times\left[1+\log\frac{1}{36}\right]-\frac{6}{36}\times\left[\log 3+\log\frac{1}{36}\right]-\frac{8}{36}\times\left[2+\log\frac{1}{36}\right]\\
&=\left(-\frac{2}{36}-\frac{4}{36}-\frac{6}{36}-\frac{8}{36}\right)\times\log\frac{1}{36}-\left(\frac{4}{36}+\frac{6}{36}\log 3+\frac{16}{36}\right)\\
&=\frac{-2-4-6-8}{36}\times\log\frac{1}{36}-\frac{4+6\log 3+16}{36}=\frac{-20}{36}\times\log\frac{1}{36}-\frac{40+6\log_2 3}{36}\\
&=3.2744\ \text{比特}
\end{aligned}
$$

可见掷两个骰子的不确定性大于掷一个骰子的不确定性。

例 10-4 对某地进行了 15 年的观察，发现 6 月份下雨的概率为 0.4，晴天的概率为 0.6；10 月份下雨的概率为 0.65，下雪的概率为 0.15，晴天的概率为 0.2，分别求它们的熵。

令 A 为 6 月份的天气状况，B 为 10 月份的天气状况。

$H(A)=-0.4\log 0.4-0.6\log 0.6\approx 0.9694$

$H(B)=-0.5\log 0.5-0.1\log 0.1-0.2\log 0.2\approx 1.2772$

$H(A)<H(B)$

但若考虑是否晴天，则有

$H(B)=0.6\log 0.6\approx 0.7204$

则 $H(B)<H(A)$

例 10-5 一电视屏幕有 576 条线，每条线有 720 个像元，故一个电视屏幕有 576×

720＝414 720 个像元，假定每个像元有 10 等级的亮度，故有$10^{414\,720}$个可能的图像，假定每个图像出现的概率相同，则有

$$H(P)=\log n=\log\left(10^{414\,720}\right)=1.4\times 10^{6}\ \text{比特}$$

例 10-6　一个图像是 4×4 的方格，其中有一方格有阴影，如图 10-3 所示，提问每一问题，只有“是”或“非”两种回答，最后确定阴影格子的位置，例如：

(1) 有阴影的格子是下面 8 个格子吗?

回答“非”，则 9～16 的格子可以略去。

(2) 有阴影的格子在左边的 4 个格子中吗?

回答“是”，则有阴影的格子在 1,2,5,6 中。

(3) 问有阴影的格子是余下的 4 个格子中底下两个吗?

回答“是”，则有阴影格子是 5 或 6。

(4) 问是左边那格子吗?

回答“非”，有阴影的格子是 6。

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

图 10-3　4×4 方格

所以问 4 个问题可以确定有阴影的格子，假定 16 个格子是有阴影格子的概率都相同，则

$$H(P)=-\sum_{i=1}^{16}\frac{1}{16}\log\frac{1}{16}=\log(16)=4$$

可见这个问题的信息量是最小问的问题数目。

其实对于每个格子有阴影的概率不一样也同样是对的。

10.5　熵的性质

先介绍关于熵的直观结果：

(1) 假定事件 A 有 n 种可能结果，其概率分别为 $p_1,p_2,\cdots,p_n$，则 $H(A)$与 $p_1,p_2,\cdots,p_n$ 的顺序无关。

(2) 已知事件 $A=X+Y$，其中 X 和 Y 是相互独立的事件。

X 有 n 种可能：$x_1,x_2,\cdots,x_n$，其概率分别是 $p_1,p_2,\cdots,p_n$。

Y 有 m 种可能：$y_1,y_2,\cdots,y_m$，其概率依次为 $q_1,q_2,\cdots,q_m$。

则 A 有 mn 种可能：$(x_1y_1,x_1y_2,\cdots,x_1y_m,x_2y_1,\cdots,x_ny_m)$。

其概率依次为 $p_1q_1,p_1q_2,\cdots,p_nq_m$。

则 $H(A)=H(X+Y)=H(X)+H(Y)$。

(3) $H(A)$当 $p_1=p_2=\cdots=p_n$ 时取极大值，当其中 $p_i=1$，其他 $p_j=0,j\neq i$ 时，$H(A)$取极小值。

(4) 事件 X 有 n 种可能，其概率分别为 $p_1,p_2,\cdots,p_n$。

$H(X)\leqslant\log n$，$H(X)\geqslant 0$；

因 $p_1=p_2=\cdots=p_n=\dfrac{1}{n}$时 $H(X)$取最大值，不确定值达到最大。

$$n\left(-\frac{1}{n}\log\frac{1}{n}\right)=-\log\frac{1}{n}=\log n$$

① $\lim_{p\to 0}(p\log p)=0$，不妨假定对数是以 e 为底 $\log_2 p=\frac{\ln p}{\ln 2}$。

证 左 $=\lim_{p\to 0}\frac{\log p}{\frac{1}{p}}=0=\lim_{p\to 0}\frac{\frac{1}{p}}{-\frac{1}{p^2}}=0=\lim_{p\to 0}(-p)=0$。

② 求 $y=-x\ln x$ 的极值。

$y'=-1-\ln x=0,\ln n=-1,x=\frac{1}{e}$。

③ 当事件 A 有 k 个可能结果：$A_1,A_2,\cdots,A_n$，其概率依次为 $p_1,p_2,\cdots,p_n,p_1+p_2+\cdots+p_n=1$，求 $H(A)=p_1\log\frac{1}{p_1}+p_2\log\frac{1}{p_2}+\cdots+p_n\log\frac{1}{p_n}$ 的极值。

根据 Lagrange 乘数法，求 $H(A)+\lambda\sum_{i=1}^{n}(p_1+p_2+\cdots+p_n)$ 的极值。

$H(A)+\lambda\sum_{i=1}^{n}(p_i)=p_1\log\frac{1}{p_1}+\cdots+p_n\log\frac{1}{p_n}+\lambda(p_1+p_2+\cdots+p_n)$，

$\frac{\partial H}{\partial p_i}+\lambda\frac{\partial}{\partial p_i}\left(\sum_{i=1}^{n}p_i\right)=-(\log p_i+1)+\lambda=0$，

$p_1=p_2=\cdots=p_n=\frac{1}{n},i=1,2,\cdots,n$。

④ $H(p_1,p_2,\cdots,p_k)=H(p_1+p_2+\cdots+p_k)+(p_1+p_2)H\left(\frac{p_1}{p_1+p_2},\frac{p_2}{p_1+p_2}\right)$。

证

$$\begin{aligned}&H(p_1+p_2+\cdots+p_k)+(p_1+p_2)H\left(\frac{p_1}{p_1+p_2},\frac{p_2}{p_1+p_2}\right)\\&=-(p_1+p_2)\log(p_1+p_2)-p_2\log p_2-\cdots-p_k\log p_k\\&\quad+(p_1+p_2)\left[\frac{p_1}{p_1+p_2}\log\frac{p_1}{p_1+p_2}+\frac{p_2}{p_1+p_2}\log\frac{p_2}{p_1+p_2}\right]\\&=-(p_1+p_2)\log(p_1+p_2)-p_3\log p_3-\cdots-p_n\log p_n\\&\quad+p_1\log(p_1+p_2)+p_2\log(p_1+p_2)-p_1\log p_1-p_2\log p_2\\&=-p_1\log p_1-p_2\log p_2-\cdots-p_n\log p_n=H(p_1,p_2,\cdots,p_n)\end{aligned}$$

还可以证明更一般的结果：

$$\begin{aligned}&H(p_{11},p_{12},\cdots,p_{1k_1},p_{21},p_{22},\cdots,p_{2k_2},\cdots,p_{n1},p_{n2},\cdots,p_{nk_n})\\&=H(p_1,p_2,\cdots,p_n)\sum_{i=1}^{n}p_iH\left(\frac{p_{i1}}{p_1},\cdots,\frac{p_{ik_1}}{p_i}\right),\end{aligned}$$

其中 $p_{ij}\geqslant 0,p_i\sum_{j=1}^{k_1}p_{ij}>0,\sum_{i=1}^{n}p_i=1$。

10.6 条 件 熵

本节考虑 U 和 V 两个互相独立的随机事件，设 U 有 k 个可能结果：$A_1,A_2,\cdots,A_k$，对应的概率为 $p(A_1),p(A_2),\cdots,p(A_k)$，$V$ 有 l 个可能结果：$B_1,B_2,\cdots,B_l$，对应的概率

为 $p(B_1),p(B_2),\cdots,p(B_l)$。

$p(A_1)+p(A_2)+\cdots+p(A_k)=1$，

$p(B_1)+p(B_2)+\cdots+p(B_l)=1$，

U、V 作为事件可能有以下的结果：

$A_1B_1,A_1B_2,\cdots,A_1B_l$，

$A_2B_1,A_2B_2,\cdots,A_2B_l$，

…

$A_kB_1,A_kB_2,\cdots,A_kB_l$。

定理 10-3：若 U、V 是相互独立的事件，则 $H(U,V)=H(U)+H(V)$。

证　$H(U,V)=-p(A_1B_1)\log p(A_1B_1)-p(A_1B_2)\log p(A_1B_2)$

$-\cdots-p(A_1B_l)\log p(A_1B_l)$

$-p(A_2B_1)\log p(A_2B_1)-\cdots-p(A_2B_l)\log p(A_2B_l)$

$-p(A_3B_1)\log p(A_3B_1)-\cdots$

$-p(A_3B_l)\log p(A_3B_l)-\cdots-p(A_kB_1)\log p(A_kB_1)$

$-\cdots-p(A_kB_l)\log p(A_kB_l)$

由于 U、V 相互独立，故 $p(A_iB_j)=p(A_i)p(B_j)$，$i=1,2,\cdots,k$，$j=1,2,\cdots,l$。

$p(A_1)+p(A_2)+\cdots+p(A_k)=1$，

$p(B_1)+p(B_2)+\cdots+p(B_l)=1$。

因此 $-p(A_1)p(B_1)[\log p(A_1)+\log p(B_1)]-p(A_1)p(B_2)[\log p(A_1)+\log p(B_2)]$

$-\cdots-p(A_k)p(B_1)[\log p(A_k)+\log p(B_1)]-\cdots$

$-p(A_k)p(B_l)[\log p(A_k)+\log p(B_l)]$

$=[-p(A_1)\log p(A_1)-p(A_2)\log p(A_2)-\cdots$

$-p(A_k)\log p(A_k)][p(B_1)+p(B_2)+\cdots+p(B_l)]$

$+[-p(B_1)\log p(B_1)-p(B_2)\log p(B_2)-\cdots$

$-p(B_l)\log p(B_l)][p(A_1)+p(A_2)+\cdots+p(A_k)]$

$=H(X)+H(Y)$

若 U 和 V 不相互独立，则有 $H(U,V)=H(U)+H(V|U)$。

$$H(UV)=-\sum_{i=1}^{k}\sum_{j=1}^{l}p(A_iB_j)\log p(A_iB_j),$$

但 $p(A_iB_j)=p(A_i)p(B_j|A_i)$，

$\log p(A_iB_j)=\log p(A_i)+\log p(B_j|A_i)$，

所以

$H(UV)=-p(A_1)p(B_1|A_1)[\log p(A_1)+\log p(B_1|A_1)]-\cdots$

$-p(A_1)p(B_l|A_1)[\log p(A_1)+\log p(B_l|A_1)]-\cdots$

$-p(A_k)p(B_1|A_k)[\log p(A_k)+\log p(B_1|A_k)]-\cdots$

$-p(A_k)p(B_l|A_k)[\log p(A_k)+\log p(B_l|A_k)]$。

另一方面：

$$p(B_1 \mid A_i) + p(B_2 \mid A_i) + \cdots + p(B_l \mid A_i)$$
$$= \frac{1}{p(A_i)}[p(A_i \mid B_1) + p(A_i \mid B_2) + \cdots + p(A_i \mid B_l)] = 1$$
$$i = 1,2,\cdots,k。$$

所以

$$H(UV) = -\sum_{i=1}^{k}\{p(A_i)[p(B_1 \mid A_i) + p(B_2 \mid A_i) + \cdots + p(B_l \mid A_i)] \cdot \log p(A_1 \mid B_l)$$
$$+ p(A_i)[p(A_i \mid B_1)\log p(A_i \mid B_1) + p(A_i \mid B_2)\log p(A_i \mid B_2)$$
$$+ \cdots + p(A_i \mid B_l)\log p(A_i \mid B_l)]\}$$
$$= -p(A_1)\log p(A_1) + p(A_1)H(V \mid A_1) + p(A_2)H(V \mid A_2)\cdots$$
$$-p(A_k)\log p(A_k) + p(A_k)H(V \mid A_k)$$

$$H(V \mid A_i) = -p(B_1 \mid A_i)\log p(B_1 \mid A_i) - p(B_2 \mid A_i)\log p(B_2 \mid A_i)$$
$$- \cdots - p(B_l \mid A_i)\log p(B_l \mid A_i),$$
$$i = 1,2,\cdots,k。$$

$$H(V \mid U) = -\sum_{i=1}^{k}\sum_{j=1}^{l} p(A_iB_j)\log p(B_j \mid A_i)$$

所以

$H(UV) = H(U) + H(V|U)$。

称 $H(V|A_i)$为已知 A_i 的条件下 V 的条件熵。

令 $H(V|U) = p(A_1)H(V|A_1) + p(A_2)H(V|A_2) + \cdots + p(A_k)H(V|A_k)$，

故若 U 和 V 不相互独立则有

$H(U,V) = H(U) + H(V|U)$。

$H(V|U)$为 U 已知条件下事件 V 的条件熵，用以度量 U 给定后留给 V 的不确定性，也称为 U 给定后留给 V 的暧昧度。

例 10-7 一种病发病率为 2%，为了诊断要做一种试验，有病的人对这种试验必有阳性反应，而健康的人阳性和阴性反应各半。设事件 V 有两种结果：B_1：健康，B_2：病人；而事件 U 的结果：A_1：阳性反应，A_2：阴性反应，求 $H(V)$，$H(V|U)$。

解 $p(B_1) = 0.98$，$p(B_2) = 0.02$，

$H(V) = -0.98\log 0.98 - 0.02\log 0.02 = 0.141$ 比特。

0.02 的人有阳性反应，0.98 的人阳性、阴性反应各半，故

$p(A_1) = 0.02 + 0.49 = 0.51$，$p(A_2) = 0.49$，

$p(B_1|A_2) = 0$，$p(B_2|A_2) = 0$，$H(V|A_2) = 0$，

$p(B_1|A_1) = \frac{49}{51}$，$p(B_2|A_1) = \frac{2}{51}$，

$H(V|A_1) = -\frac{49}{51}\log\frac{49}{51} - \frac{2}{51}\log\frac{2}{51} = 2.2354$ 比特，

$H(V|U) = 0.51 \times 0.2354 = 0.1201$，

即试验结果使 V 的不确定性从 0.141 下降到 0.1201。

例 10-8　一盒子有 5 个黑球和 10 个白球，X 随机从中抽取一球，不放回去，Y 随机抽取第二球。

(1) X 抽球的不确定性有多少？

(2) X 抽的球是黑的，Y 的不确定性是多少？

(3) X 抽的球是白的，Y 的不确定性是多少？

(4) Y 的不确定性是多少？

解：

(1) $p(w_x)=\frac{10}{15}=\frac{2}{3}, p(b_x)=\frac{5}{15}=\frac{1}{3}$，

$H(x)=-\frac{1}{3}\log\frac{1}{3}-\frac{2}{3}\log\frac{2}{3}=0.92$ 比特。

(2) 若 X 抽到的球是黑的：

$p(b_y|b_x)=\frac{4}{14}=\frac{2}{7}, p(b_y|b_x)=\frac{10}{14}=\frac{5}{7}$，

$H(Y|b_x)=-\frac{2}{7}\log\frac{2}{7}-\frac{5}{7}\log\frac{5}{7}=0.86$ 比特。

(3) 若 X 抽到的是白球：

$p(b_y|w_x)=\frac{5}{14}, p(w_y|w_x)=\frac{9}{14}$，

$H(Y|w_x)=-\frac{5}{14}\log\frac{5}{14}-\frac{9}{14}\log\frac{9}{14}=0.94$ 比特。

(4) $H(Y|X)=p(b_x)H(Y|b_x)+p(w_x)H(Y|w_x)=\frac{1}{3}\times 0.86+\frac{2}{5}\times 0.94=0.91$ 比特。

例 10-9　一盒子里放 n 个球，其中 m 个是红球，$n-m$ 个是白球，事件 U 是从中随机取出第一个球，V 是从中取出第二个球，求 $H(U)$ 和 $H(V)$，$H(U|V)$，$H(V|U)$。

解：U 有两种结果：u_1 取的是红球，u_2 取的是白球。

V 有两种结果：v_1 取的是红球，v_2 取的是白球。

事件 V 是取第二个球，而第一个球可能是红的，也可能是白的，故有

$$p(u_1)=\frac{m}{n}, p(u_2)=\frac{n-m}{n},$$

$$H(U)=-\frac{m}{n}\times\log\frac{m}{n}-\frac{n-m}{n}\times\log\frac{n-m}{n},$$

$$p(v_1)=\frac{m}{n}\times\frac{m-1}{n-1}+\frac{n-m}{n}\times\frac{m}{n-1}=\frac{m}{n},$$

$$p(v_2)=\frac{m}{n}\times\frac{n-m}{n}+\frac{n-m}{n}\times\frac{n-m-1}{n-1}=\frac{n-m}{n},$$

故 $H(U)=H(v)$。

若已知 U 或 V 的结果，例如已知第一个球是白球，则第二个球是白球的概率是

$p(v_1 \mid u_1)=\frac{m-1}{n-1}, p(v_2 \mid u_1)=\frac{n-m}{n-1},$

$p(v_1 \mid u_2)=\frac{m}{n-1}, p(v_2 \mid u_2)=\frac{n-m-1}{n-1}$,从而

$H(V \mid u_1)=-\frac{m-1}{n-1}\times\log\frac{m-1}{n-1}-\frac{n-m}{n-1}\times\log\frac{n-m}{n-1},$

$H(V \mid u_2)=-\frac{m}{n-1}\times\log\frac{m}{n-1}-\frac{n-m-1}{n-1}\times\log\frac{n-m-1}{n-1},$

若 $m<n-m$,则

$H(V \mid u_1)<H(v), H(V \mid u_2)>H(v)$。

即当红球数目 $m<n-m$,若第一个球已知是红球时,事件 V 的不确定性减少了,极而言之,若 $m=1$,已知第一个球是红球,则第二个球无疑是白球,$H(V)$是不存在不确定性的。

定理 10-4:$H(U)-H(U \mid V)=H(V)-H(V \mid U)$。

证　根据公式:

$H(U,V)=H(U)+H(V \mid U),$

$H(U,V)=H(V)+H(U \mid V)$。

设事件 U 可能出现的结果:$A_1, A_2, \cdots, A_k$;事件 V 可能出现的结果:$B_1, B_2, \cdots, B_l$;则

$$\begin{aligned} H(U)-H(U \mid V) = H(V)-H(V \mid U) \\ &= p(A_1B_1)\log\frac{p(A_1B_1)}{p(A_1)p(B_1)}+p(A_1B_2)\log\frac{p(A_1B_2)}{p(A_1)p(B_2)} \\ &\quad+\cdots+p(A_kB_l)\log\frac{p(A_kB_l)}{p(A_k)p(B_l)} \\ &= \sum_{i=1}^{k}\sum_{j=1}^{l} p(A_iB_j)\frac{p(A_iB_j)}{p(A_i)p(B_j)} \end{aligned}$$

其中 $p(A_i)$表示 A_i 出现的概率,以此类推。

因 $H(U)=-p(A_1)\log p(A_1)-p(A_2)\log p(A_2)-\cdots-p(A_k)\log p(A_k),$

$H(V)=-p(B_1)\log p(B_1)-p(B_2)\log p(B_2)-\cdots-p(B_l)\log p(B_l),$

$H(U,V)=\sum_{i=1}^{k}\sum_{j=1}^{l} p(A_iB_j)\log p(A_iB_j)$。

另一方面:

$p(A_i)=p(A_iB_1)+p(A_iB_2)+\cdots+p(A_iB_l),$

故 $-p(A_i)\log p(A_i)=-p(A_iB_1)\log p(A_i)-p(A_iB_2)\log p(A_i)+\cdots+p(A_iB_l)\log p(A_i),$

$i=1,2,\cdots,k,$

$H(U)=-\sum_{i=1}^{k}[p(A_iB_1)+p(A_iB_2)+\cdots+p(A_iB_l)]\log p(A_i)$

$$H(V) = -\sum_{j=1}^{l}[p(A_1B_j) + p(A_2B_j) + \cdots + p(A_kB_j)]\log p(B_j)$$

$$\begin{aligned} H(U) - H(U \mid V) = & -p(A_1B_1)\ [\log p(A_1) + \log p(B_1) - \log p(A_1B_1)] \\ & - p(A_1B_2)[\log p(A_1) + \log p(B_2) - \log p(A_1B_2)] - \cdots \\ & - p(A_kB_l)[\log p(A_k) + \log p(B_l) - \log p(A_kB_l)] \\ = & \sum_{i=1}^{k}\sum_{j=1}^{l} p(A_iB_j)\ \frac{p(A_iB_j)}{p(A_i)p(B_j)} \end{aligned}$$

定义 10-2：$I(U,V) = H(V) - H(V \mid U)$。

用 $I(U,V)$来度量 V 和 U 的依赖程度，当 U 和 V 彼此独立，则 $I(U,V)=0$。

如若 U 和 V 完全相关，则 $I(U,V)=H(V)$，称 $I(U,V)$为交互熵。

用 Venn 图表示 $H(U)$，$H(V)$和 $I(U,V)$的关系如图 10-4 所示。

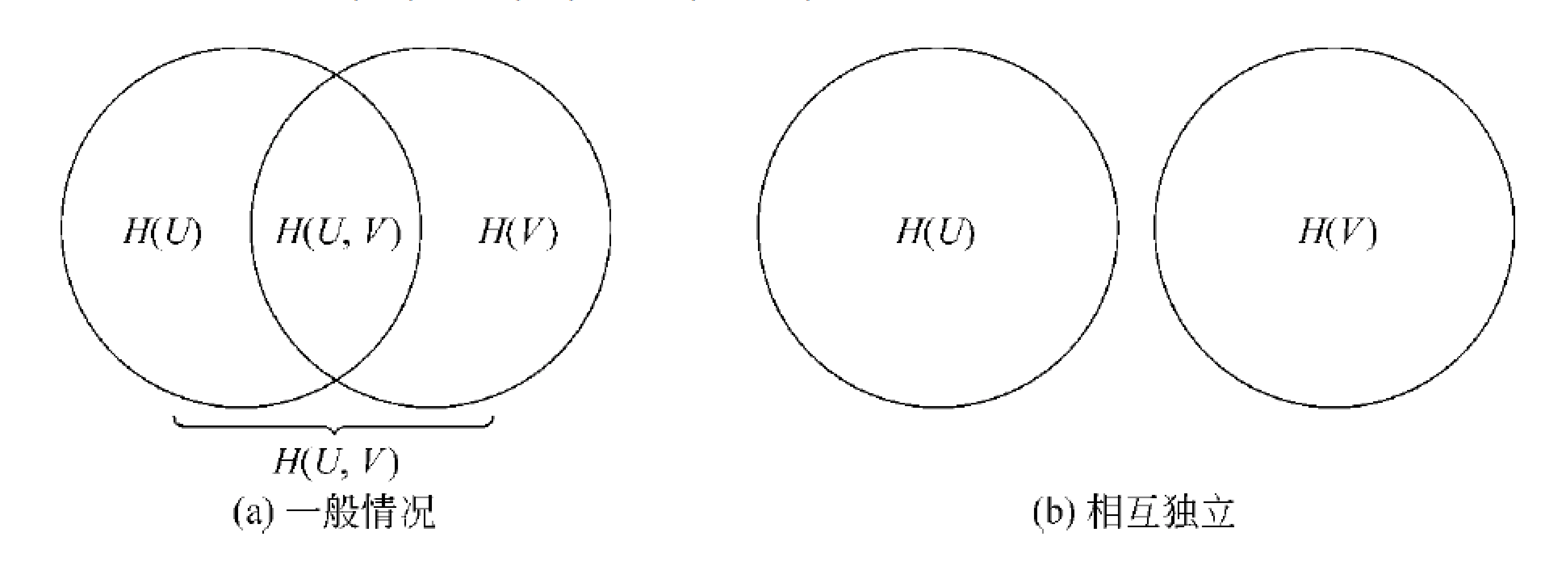


图 10-4　$H(V)$和 $I(U,V)$的关系

(1) $H(V \mid U) \leqslant H(U)$，$H(U \mid V) \leqslant H(V)$。

(2) $H(U) \geqslant I(U,V)$，$H(V) \geqslant I(U,V)$。

(3) $H(U,V) = H(U \mid V) + I(U,V) + H(V \mid U) = H(V) + H(U \mid V) = H(U) + H(V \mid U)$。

(4) $H(U,V) \leqslant H(U) + H(V)$。

(5) 若 U 和 V 相互独立，则 $I(U,V)=0$，$H(U,V)=H(U)+H(V)$，

$H(U)=H(U \mid V)$，$H(V)=H(V \mid U)$。

例 10-10　二元信道，设$\overline{p_0}$是输入端输入 0，经过传输过程出错的概率；$\overline{p_1}$是输入 1，传输出错的概率。设$\overline{p_0}=\frac{1}{3}$，$\overline{p_1}=\frac{2}{5}$，输入 0 的正确率为 $1-\frac{1}{3}=\frac{2}{3}$，输入 1 的正确率为 $1-\frac{2}{5}=\frac{3}{5}$。现在已知输入端 X 的概率颁：0 的概率为 $p_0=\frac{1}{4}$，1 的概率为$\frac{3}{4}$，求输出端 Y 的概率分布。

令输出端 0 的概率为 q_0，输出端为 1 的概率为 q_1。

$q_0 = p_0P(y=0 \mid x=0) + p_1P(y=0 \mid x=1)$，

$q_1 = p_0P(y=1 \mid x=0) + p_1P(y=1 \mid x=1)$，

$P(y=0 \mid x=1)$表示输入为 1，而输出为 0 的概率，其他以此类推。

$P(y=0 \mid x=0) = 1-\frac{1}{3}=\frac{2}{3}$，$P(y=1 \mid x=0)=\frac{1}{3}$，

$P(y=0 \mid x=1)=\frac{2}{5}, P(y=1 \mid x=1)=1-\frac{2}{5}=\frac{3}{5}$，

所以

$q_0=\frac{1}{4}\times\frac{2}{3}+\frac{3}{4}\times\frac{2}{5}=\frac{1}{6}+\frac{9}{10}=\frac{14}{30}=\frac{7}{15}$，

$q_1=\frac{1}{4}\times\frac{1}{3}+\frac{3}{4}\times\frac{3}{5}=\frac{1}{12}+\frac{9}{20}=\frac{32}{60}=\frac{8}{15}$，

$H(X)=-p_0\log p_0-p_1\log p_1=-\frac{1}{4}\log\frac{1}{4}-\frac{3}{4}\log\frac{3}{4}=0.811$ 比特。

$H(y)=-q_0\log q_0-q_1\log q_1=-\frac{7}{15}\log\frac{7}{15}-\frac{8}{15}\log\frac{8}{15}=0.997$ 比特。

(X,Y)的分布：

(1) $(0,0)$状态的概率，即发送 0，接收也是 0 的概率：

$$p_{00}=p_0P(y=0 \mid x=0)=\frac{1}{4}\times\frac{2}{3}=\frac{1}{6}。$$

(2) $(0,1)$状态的概率：

$$p_{01}=p_0P(y=1 \mid x=0)=\frac{1}{4}\times\frac{1}{3}=\frac{1}{12}。$$

(3) $(1,0)$状态的概率：

$$p_{10}=p_1P(y=0 \mid x=1)=\frac{3}{4}\times\frac{2}{5}=\frac{3}{10}。$$

(4) $(1,1)$状态的概率：

$$p_{11}=p_1P(y=1 \mid x=1)=\frac{3}{4}\times\frac{3}{5}=\frac{9}{20}，$$

$$H(X,Y)=-\frac{1}{6}\log\frac{1}{6}-\frac{1}{12}\log\frac{1}{12}-\frac{3}{10}\log\frac{3}{10}-\frac{9}{20}\log\frac{9}{20}=1.769 \text{ 比特。}$$

条件熵：

$$\begin{aligned}H(Y \mid x=0)&=-P(y=0 \mid x=0)\log P(y=0 \mid x=0)\\&\quad-P(y=1 \mid x=0)\log P(y=1 \mid x=0)\\&=-\frac{2}{3}\log\frac{2}{3}-\frac{1}{3}\log\frac{1}{3}=0.918 \text{ 比特；}\end{aligned}$$

$$\begin{aligned}H(Y \mid x=1)&=-P(y=0 \mid x=1)\log P(y=0 \mid x=1)\\&\quad-P(y=1 \mid x=1)\log P(y=1 \mid x=1)\\&=-\frac{2}{5}\log\frac{2}{5}-\frac{3}{5}\log\frac{3}{5}=0.971 \text{ 比特；}\end{aligned}$$

$$\begin{aligned}H(Y \mid X)&=p_0H(Y \mid x=0)+p_1H(Y \mid x=1)\\&=\frac{1}{4}\times0.918+\frac{3}{4}\times0.971=0.2295+0.7282=0.9577 \text{ 比特。}\end{aligned}$$

例 10-11　设投掷一均匀的骰子，若出现 1，2，3，4，则掷银币一次，若出现 5，6，则掷银币两次，试从银币出正面的次数，求骰子投掷的信息量。

骰子出现 1,2,3,4,5,6 的概率都是$\frac{1}{6}$,银币出正反面的概率都是$\frac{1}{2}$,由骰子出 1,2,3,4,掷银币仅一次,故出现两次正面和两次反面的概率是 0,骰子出 5,6,掷银币两次,故出正面或反面的概率都是$\left(\frac{1}{2}\right)^2=\frac{1}{4}$。

图 10-5 中 Y_1 表示银币正面出现 0 次($y=0$)的状态,Y_2,Y_3 分别表出银币正面次数依次为 1,2。如图 10-5 所示以此类推。

图 10-5　状态转移

$$P(X=0)=\frac{4}{6}=\frac{2}{3},P(X=1)=\frac{1}{3},$$

$$P(Y=0|X=0)=\frac{1}{2},P(Y=1|X=0)=\frac{1}{2},$$

$$P(Y=2|X=0)=0,P(Y=0|X=1)=\frac{1}{4},$$

$$P(Y=1|X=1)=\frac{1}{2},P(Y=2|X=1)=\frac{1}{4}$$

$$H(Y|X=0)=-P(Y=0|X=0)\log P(Y=0|X=0)-P(Y=1|X=0)\log P(Y=1|X=0)-P(Y=2|X=0)\log P(Y=2|X=0)=-\frac{1}{2}\log\frac{1}{2}-\frac{1}{2}\log\frac{1}{2}=1。$$

$$\begin{aligned}H(Y|X=1)&=-\frac{1}{4}\log\frac{1}{4}-\frac{1}{2}\log\frac{1}{2}-\frac{1}{4}\log\frac{1}{4}=-\frac{1}{2}\times\left(\log\frac{1}{4}-\log\frac{1}{2}\right)\\&=\frac{1}{2}\times(2+1)=\frac{3}{2},\end{aligned}$$

$$\begin{aligned}H(Y|X)&=P(X=0)H(Y|X=0)+P(X=1)H(Y|X=1)\\&=\frac{2}{3}+\frac{1}{3}\times\frac{3}{2}=\frac{2}{3}+\frac{1}{2}=\frac{7}{6}=1.166,\end{aligned}$$

同时因

$$\begin{aligned}P(Y=0)&=P(Y=0|X=0)P(X=0)+P(Y=0|X=1)P(X=1)\\&=\frac{1}{2}\times\frac{2}{3}+\frac{1}{4}\times\frac{1}{3}=\frac{1}{3}+\frac{1}{12}=\frac{5}{12},\end{aligned}$$

$$\begin{aligned}P(Y=1)&=P(Y=1|X=0)P(X=0)+P(Y=1|X=1)P(X=1)\\&=\frac{1}{2}\times\frac{2}{3}+\frac{1}{2}\times\frac{1}{3}=\frac{1}{2},\end{aligned}$$

$$\begin{aligned}P(Y=2)&=P(Y=2|X=0)P(X=0)+P(Y=2|X=1)P(X=1)\\&=\frac{1}{4}\times\frac{1}{3}=\frac{1}{12},\end{aligned}$$

$$H(Y)=-\frac{5}{12}\log\frac{5}{12}-\frac{1}{2}\log\frac{1}{2}-\frac{1}{12}\log\frac{1}{12}=1.325\text{ 比特。}$$

10.7　信道容量

假定信道输入端的输入字符集:

$$\sum\nolimits_1 = \{x_1, x_2, \cdots, x_m\}$$

输出端输出的字符集：

$$\sum\nolimits_2 = \{y_1, y_2, \cdots, y_m\}$$

若输入端输入一序列：$X_1, X_2, \cdots, X_k, \cdots$，

若序列中元素 X_i 为 x_j 的概率只与 x_j 有关，即

$$P(X_i = x_j) = p_j$$

与序数 i 无关，则称该发出端为无记忆的信号源。

若 $(X_1, X_2, \cdots)$ 是属于 $\sum_1$ 的输入序列，$(Y_1, Y_2, \cdots)$ 是属于 $\sum_2$ 的输出序列，而条件概率 $P(Y_k = y_j \mid X_i = x_j)$ 与 k 无关，则称该信道为无记忆信道，二元对称信道矩阵

$$\boldsymbol{P} = (p_{ij})_{2\times 2}$$

$$p_{ij} = p_{ji}, i, j = 1, 2$$

关于交互信息 $I(X,Y)$

$I(X,Y) = H(X) + H(Y) - H(X,Y)$。

因为 $H(X,Y) = H(Y,X)$，

所以 $I(X,Y) = I(Y,X)$。

对于二元的对称信道有

$I(X,Y) = H(Y) - H(Y|X)$，

其中 $X = \{a_1, a_2\}, Y = \{b_1, b_2\}, a_1 = 0, a_2 = 1, b_1 = 0, b_2 = 1$，

故 $H(Y \mid X) = \sum_{i=1}^{2}\sum_{j=1}^{2} p(a_i, b_j)\log\frac{1}{p(b_j \mid a_i)}$。

由于 $p(a_i, b_j) = p(a_i)p(b_j|a_i)$

所以

$$\begin{aligned}
H(Y \mid X) &= \sum_{i=1}^{2} p(a_i)\sum_{j=1}^{2} p(b_j \mid a_i)\log\frac{1}{p(b_j \mid a_i)} \\
&= \sum_{i=1}^{2} p(a_i)\left[p(0 \mid a_i)\log\frac{1}{p(0 \mid a_i)} + p(1 \mid a_i)\log\frac{1}{p(1 \mid a_i)}\right] \\
&= p(0)\left[p(0 \mid 0)\log\frac{1}{p(0 \mid 0)} + p(1,0)\log\frac{1}{p(1 \mid 0)}\right] \\
&\quad + p(1)\left[p(0 \mid 1)\log\frac{1}{p(0 \mid 1)} + p(1,1)\log\frac{1}{p(1 \mid 1)}\right] \\
&= p(0)\left[q\log\frac{1}{q} + p\log\frac{1}{p}\right] + p(1)\left[q\log\frac{1}{q} + p\log\frac{1}{p}\right] \\
&= (p(0) + p(1))\left[p\log\frac{1}{p} + q\log\frac{1}{q}\right] = p\log\frac{1}{p} + q\log\frac{1}{q} \\
&= H(p, 1-p)
\end{aligned}$$

其中 $q = 1 - p, p(0) + p(1) = 1$。

平均交互信息 $I(X,Y)$ 为传输一个符号经信道的平均信息量，也可以认为它是信道的传输率 R，即

$$R = I(X,Y)\frac{\text{比特}}{\text{信道符号}}$$

它和信道传输特性 $p(y_j|x_i)$ 有关，又和发送端的统计特性 $p(x_i)$ 有关，$i=1,2,\cdots,m$，$j=1,2,\cdots,n$。研究信道本身希望找到一个量，用来表征信道本身的传输信息的最大能力。

定义 10-3：$C=\max\limits_{p(x)}\{I(X,Y)\}$，称为信道容量。

信道容量是对具体信道的最大信息传输率，是对信道传输信息能力的一种度量，计算各种类型信道的信道容量是十分复杂的过程，我们仅限于讨论比较重要的二元对称信道。

由定义可知不可能有超过信道容量 C 的 $I(X,Y)$。

定理 10-5：对于二元对称信道，若其传输错误概率为 $p\left(<\frac{1}{2}\right)$，则其信道容量

$C(p)=1+p\log p+(1-p)\log(1-p)$。

证 设输入 X 的概率分布为输入 0 的概率为 α，则输入 1 的概率为 $\beta=1-\alpha$，则输出 0 的概率为 $\alpha(1-p)+\beta p$，输出 1 的概率为 $(1-\alpha)(1-\beta)+\alpha p=\beta(1-p)+\alpha p$，也就是输出 0 由两部分组成，一是 0 发送正确传输；另一部分是发送 1，但传输出错引起的；输出 1 也一样由两部分组成：

$$H(X,Y)=p(0|0)\log\frac{1}{p(0|0)}+p(0|1)\log\frac{1}{p(0|1)}+p(1,0)\log\frac{1}{p(1|0)}+p(1,1)\log\frac{1}{p(1|1)},$$

$p(0,0)=\alpha(1-p)$，$p(0,1)=\alpha p$，$p(1,0)=(1-\alpha)p$，$p(1,1)=(1-\alpha)(1-p)$。

令 $q=1-p$。

$$\begin{aligned}H(X,Y)=&-(1-p)\alpha\log[\alpha(1-p)]-\alpha p\log[\alpha p]\\&-\beta(1-p)\log[\beta(1-p)]-\beta p\log[\beta p]\\=&-\alpha q\log\alpha-\alpha q\log q-\alpha p\log\alpha-\alpha p\log p-\beta q\log\beta-\beta q\log q-\beta p\log\beta-\beta p\log p\\=&-\alpha(p+q)\log\alpha-(\alpha+\beta)q\log q-\beta(p+q)\log\beta-(\alpha+\beta)p\log p\\=&-\alpha\log\alpha-\beta\log\beta-p\log p-q\log q\end{aligned}$$

$$H(X)=\alpha\log\frac{1}{\alpha}+\beta\log\frac{1}{\beta}$$

$$H(Y)=(\alpha q+\beta p)\log\frac{1}{(\alpha q+\beta p)}+(\beta q+\alpha p)\log\frac{1}{(\beta q+\alpha p)}$$

所以
$$\begin{aligned}I(X,Y)=&-\alpha\log\alpha\beta q+\alpha p-(\alpha q+\beta p)\log(\alpha q+\beta p)-(\beta q+\alpha p)\log(\beta q+\alpha p)\\&-[-\alpha\log\alpha-\beta\log\beta-p\log p-q\log q]\\=&\,p\log p+q\log q-(\alpha q+\beta p)\log(\alpha q+\beta p)-(\beta q+\alpha p)\log(\beta q+\alpha p),\end{aligned}$$

由于 $\beta=1-\alpha$

$$\frac{\mathrm{d}I}{\mathrm{d}\alpha}=-(q-p)(\alpha q+\beta p)-(q-p)-(p-q)\log(\beta q+\alpha p)-(p-q)$$

$$=(p-q)\log\frac{\alpha q+\beta p}{\beta q+\alpha p}=0,\text{即 }\alpha q+\beta p=\beta q+\alpha p,$$

$(\alpha-\beta)q=(\alpha-\beta)p$，$(\alpha-\beta)=0$，$\alpha+\beta=1$

所以 $\alpha=\beta=\frac{1}{2}$，以之代入 $I(X,Y)$，得

$C=1+p\log p+(1-p)\log(1-p)$作为 p 的函数在区间$\left[0,\frac{1}{2}\right]$上是单调减函数,而且 $C(0)=1, C\left(\frac{1}{2}\right)=0$。

对于二元对称信道假定 0 的输入概率为 p_0,1 的输入概率为 $p_1=1-p_0$,信道出错为 p,则输出 0 和 1 的概率 q_0 和 q_1,

$q_0=p_0P+\overline{p_0}\,\overline{P}, q_1=p_0\overline{P}+\overline{p_0}P$,

$(q_0,q_1)=(p_0,\overline{p_0})\begin{vmatrix} P & \overline{P} \\ \overline{P} & P \end{vmatrix}$,

可证 $q_1=\overline{q_0}=1-q_0$。

令 $Q_{00}=P(x=0|y=0), Q_{01}=P(x=0|y=1)$,

$Q_{10}=P(x=1|y=0), Q_{11}=P(x=1|y=1)$,

即 Q_{ij} 为已知,输出为 j 的条件下输出为 i 的概率,其中 $i,j=0,1$,

由于

$p_iP(y_j|x_i)=P(x_i,y_j)=P(y_j)P(x_i|y_j)=q_jQ_{ij}$

或展开为

$Q_{00}=\dfrac{p_0P}{p_0P+\overline{p_0}\,\overline{P}}, Q_{01}=\dfrac{p_0\overline{P}}{p_0\overline{P}+\overline{p_0}P}, Q_{10}=\dfrac{\overline{p_0}\,\overline{P}}{p_0\overline{P}+\overline{p_0}\,\overline{P}}, Q_{11}=\dfrac{\overline{p_0}\,P}{p_0\overline{P}+\overline{p_0}\,\overline{P}}$,

假定$P=0.8, p_0=0.5, \overline{P}=0.2, \overline{p_0}=0.5$,

$q_0=0.5\times0.8+0.5\times0.2=0.5$,

$q_1=0.5\times0.2+0.5\times0.8=0.5$,

$Q_{10}=\dfrac{0.5\times0.8}{0.5}=0.8, Q_{01}=\dfrac{0.5\times0.2}{0.5}=0.2$,

$Q_{10}=\dfrac{0.5\times0.2}{0.5}=0.2, Q_{11}=\dfrac{0.5\times0.8}{0.5}=0.8$。

10.8 无噪声信道

无噪声信道也就是没有干扰的信道,既然无干扰,就不考虑纠错、检错,主要考虑编码通信的效率问题。它的编码可以形式化地定义为由字符集$\{a_1,a_2,\cdots,a_n\}$的元素到$\sum^*$的映射,$\sum^*$是由某字符集中的字符构成的字符串。

设信息 $m=m_1m_2\cdots m_k$,映射 f 作用于 m 得

$$f(m)=f(m_1)f(m_2)\cdots f(m_k)$$

即对 $m_1m_2\cdots m_k$ 依顺序编码,然后串接起来,但对映射 f 要求能唯一地译码。$f(m_i)$称为 m_1 对应的码字,$|f(m_i)|$称为码字的长度。令

$$l=\sum_{i=1}^{k}p_i\,|\,f(m_i)\,|$$

称为编码 f 的编码的平均长度。p_i 是 m_i 出现的概率。

所有码长都相同的编码称为定长码,如 ASCII 码便是定长码。长度不等的编码则要求不存在 m_i 和 m_j 使 $f(m_i)$是 $f(m_j)$的字首,也就是 $f(m_i)$不是 $f(m_j)$的前头一部分。

对于任意连接起来的码字序列,先看一个例子。

例 10-12　$\sum=\{0,1\}$,5 个信息字 m_1,m_2,m_3,m_4,m_5 的编码

$f(m_1)=0,f(m_2)=10,f(m_3)=110,f(m_4)=1110,f(m_5)=1111$,

如图 10-6 所示用二分树来说明就很清楚了。5 个编码是二分树的 5 个"叶子",如图 10-6 所示。

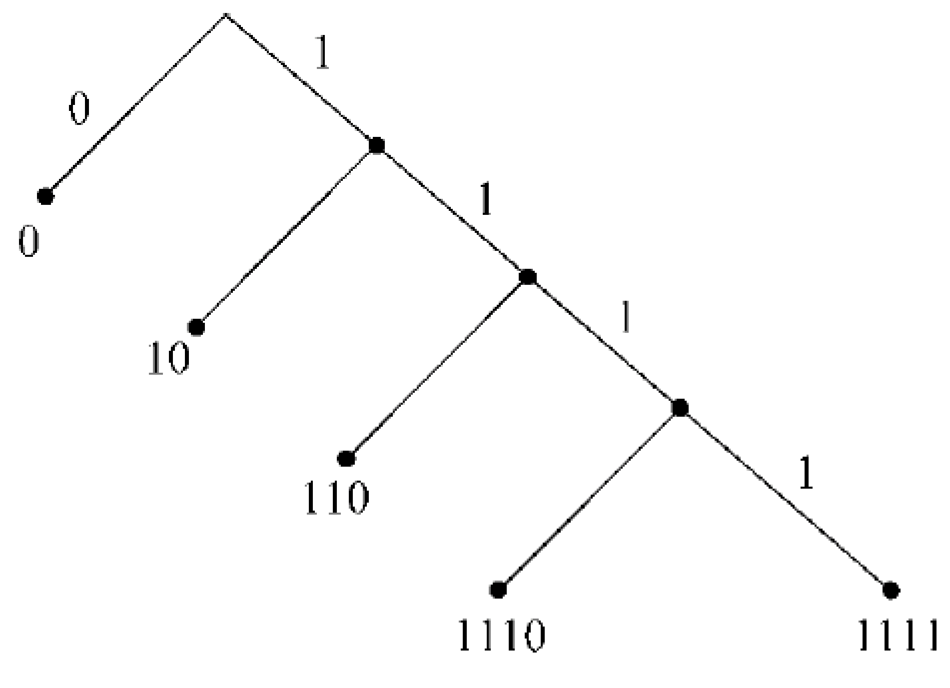


图 10-6　用二叉树说明

Kraft 不等式:d 元码 C,设有长度分别为 $l_1,l_2,\cdots,l_n$ 的码字为唯一可译码的充分条件是

$$\sum_{i=1}^{n} d^{-l_i} \leqslant 1$$

证　不妨假定 $l_1\leqslant l_2\leqslant\cdots\leqslant l_n$,或更进一步 l 个不同长度 $l_i=i$ 的码字分别有 n_i 个,$i=1,2,\cdots,l$ 即

$$\sum_{i=1}^{l} n_i d^{-i} \leqslant 1$$

即 $n_1d^{-1}+n_2d^{-2}+\cdots+n_ld^{-l}\leqslant 1$。

对上式同时乘以 d^l 得

$n_1d^{l-1}+n_2d^{l-2}+\cdots+n_ld^0\leqslant d^l$,

$n_l\leqslant d_l-n_1d^{-1}-n_2d^{-2}-\cdots-n_{l-1}d^1$。

同理

$n_1d^{l-2}+n_2d^{l-3}+\cdots+n_{l-1}+n_ld^{-1}\leqslant d^{l-1}$,

$n_{l-1}\leqslant d^{l-1}-n_1d^{l-2}-n_2d^{l-3}-\cdots-n_{l-2}d-n_ld^{-1}\leqslant d^{l-1}-n_1d^{l-2}-n_2d^{l-3}-\cdots-n_{l-2}d$

$n_{l-2}\leqslant d^{l-2}-n_1d^{l-3}-\cdots-n_{l-3}d$,

…

$n_3\leqslant d^3-n_1d^2-n_2d$,

$n_2\leqslant d^2-n_1d$,

$n_1\leqslant d$。

这一组不等式对构造变长度码起到关键作用。

首先从 d 个字符集 A 中选出 n_1 个字符,构造长度为 1 的码字。还剩有 $d-n_1$ 个字

符，故有$(d-n_1)d$个长度为2的字符串与第一组从d个字符中选出n_1个字符作为长度为1的码，不存在第二组码字是第一组码字的延续。

用类似办法可从$(d^2-n_1d-n_2)d$中选出n_3个长度为3的符号串，作为长度为3的码字，这个第三组码都不存在是前面两组码的延续问题，以此类推保证长度依次为1，2，…，l的唯一可译码的存在。

例 10-13 二元信道$(d=2)$，信源的字符集$A=\{a_1,a_2,a_3,a_4\}$，已知$p(a_1)=\frac{1}{2}$，$p(a_2)=\frac{1}{4}$，$p(a_3)=p(a_4)=\frac{1}{8}$，码长依次为$n_1=1,n_2=2,n_3=3,n_4=3$：

$$2^{-1}+2^{-2}+2^{-3}+2^{-3}=\frac{1}{2}+\frac{1}{4}+\frac{2}{8}=1$$

故存在这样的唯一可译码，使出现概率高的码短，出现概率低的码长。

10.9 无噪声无记忆的编码理论

信道输入字符集$A=\{a_1,a_2,\cdots,a_d\}$，为了便于在信道上传输必须对信源$S=\{s_1,s_2,\cdots,s_n\}$进行编码，假定码长分别为$l_1,l_2,\cdots,l_n$，根据Kraft不等式为$\sum_{i=1}^{n}d^{-l_i}\leqslant 1$，则存在唯一可译码，令

$$l=p(s_1)l_1+p(s_2)l_2+\cdots+p(s_n)l_n=\sum_{i=1}^{n}p(s_i)l_i$$

熵为$H(S)=-p(s_1)\log p(s_1)-p(s_1)\log p(s_1)-\cdots-p(s_n)\log p(s_n)=$

$$-\sum_{i=1}^{n}p(s_i)\log p(s_i)$$

定理 10-6：一个无记忆信源$S=\{s_1,s_2,\cdots,s_n\}$，熵为$H(S)$，编码字符集A的元素个数为d，即$A=\{a_1,a_2,\cdots,a_d\}$，则存在唯一可译码，使

$$\frac{H(S)}{\log d}\leqslant\bar{l}\leqslant\frac{H(S)}{\log d}+1,$$

证明
$$\begin{aligned}H(S)-\bar{l}\log d&=-\sum_{i=1}^{n}p(s_i)\log p(s_i)-\left[\sum_{i=1}^{n}p(s_i)l_i\right]\log d\\&=-\sum_{i=1}^{n}p(s_i)\log p(s_i)+\sum_{i=1}^{n}p(s_i)\log d^{-l_i}\\&=-\sum_{i=1}^{n}p(s_i)\log\frac{d^{-l_i}}{p(s_i)}\\&\leqslant\log\left[\sum_{i=1}^{n}p(s_i)\frac{d^{-l_i}}{p(s_i)}\right],\text{即}\sum_{i=1}^{n}p(s_i)\frac{d^{-l_i}}{p(s_i)}\leqslant 0\end{aligned}$$

所以$\bar{l}\geqslant\frac{H(S)}{\log d}$。

其中$\sum_{i=1}^{n}p(s_i)\frac{d^{-l_i}}{p(s_i)}\leqslant\log\left[\sum_{i=1}^{n}p(s_i)\frac{d^{-l_i}}{p(s_i)}\right]$是由对数函数的上凸性质所决定的，如图10-7所示。

其中 $y_1=p\log a+(1-p)\log b, y_2=\log[p(a)+(1-p)b], y_2>y_1$，

即 $\log[p(a)+(1-p)b]>p\log a+(1-p)\log b$，

后面证

$$\bar{l}<\frac{H(S)}{\log d}+1$$

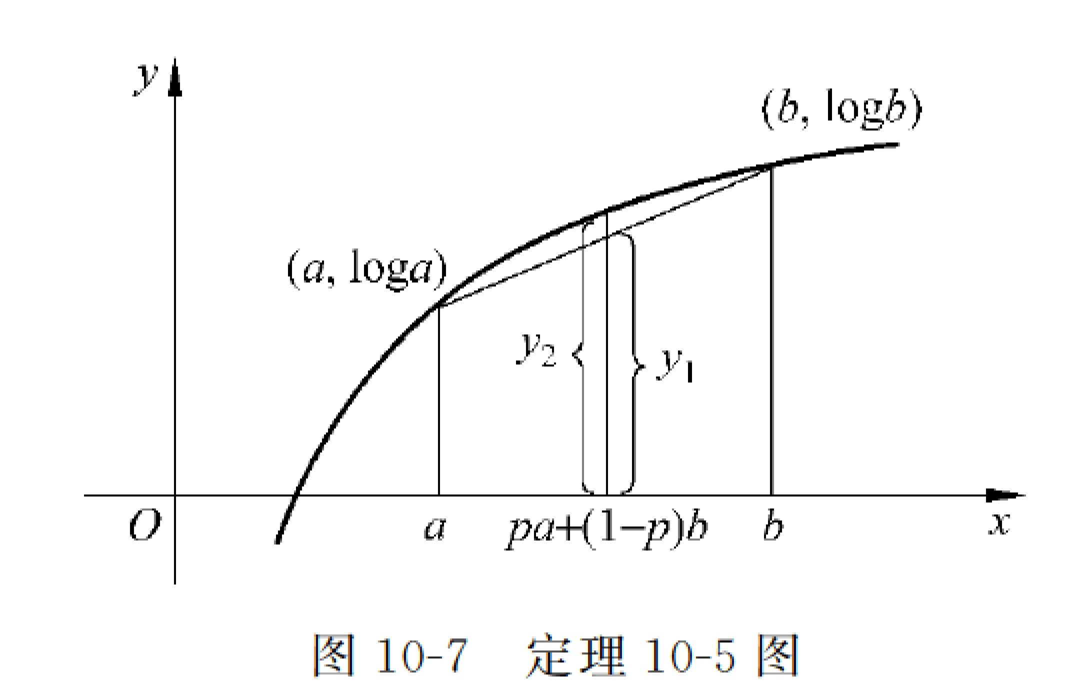


图 10-7　定理 10-5 图

假定取 l_i 满足

$$-\log p(s_i)\leqslant l_i\leqslant -\log p(s_i)+1$$

$$\frac{1}{p(s_i)}\leqslant d^{l_i}\leqslant\frac{d}{p(s_i)}$$

$$\sum_{i=1}^{n}p(s_i)\geqslant d^{l_i}\geqslant\sum_{i=1}^{n}\frac{p(s_i)}{d}$$

由于 $\sum_{i=1}^{n}p(s_i)=1$，所以 $\bar{l}<\frac{H(S)}{\log d}+1$。

10.10　Huffman 码

下面仅就二元码予以讨论，即 $d=2, A=\{0,1\}$。

假定有 $(w_1,w_2,\cdots,w_n)$，n 个字需要编码，w_i 的出现概率为 $p_i, i=1,2,\cdots,n$，$p_1+p_2+\cdots+p_n=1$。

所谓最佳编码问题即求使平均码长 $\bar{l}=\sum_{i=1}^{n}p_il_i$ 达到最小。

一组编码可对应一棵二元树 T，若 v_i 分别对应一权使 v_i 到树根的长度为 l_i，因此设计最佳编码是找一棵二元编码树，使得期望值 $m(T)=\sum_{i=1}^{n}p_il_i$ 达到最小。其中 $\sum_{i=1}^{n}$ 是对码树的“叶片”求和，这样又叫 Huffman 树，假定 $p_1\leqslant p_2\leqslant\cdots\leqslant p_n$。

首先证明，设 T^* 是带权 $p_1,p_2,\cdots,p_n$ 的最优二分树，则 p_1,p_2 必定是一对“兄弟”，因 p_1 最小，故与之对应的 l_i 最大，同时 p_1 不可能没有“兄弟”节点，如若不然可缩短它的 l_i 使 $m(T)$ 更小与 $m(T)$ 达到最小的假定相矛盾。

若将 p_1+p_2 的值赋给它们共同的“父亲”节点，得一 $n-1$ 个节点的树 T_{n-1}^*。

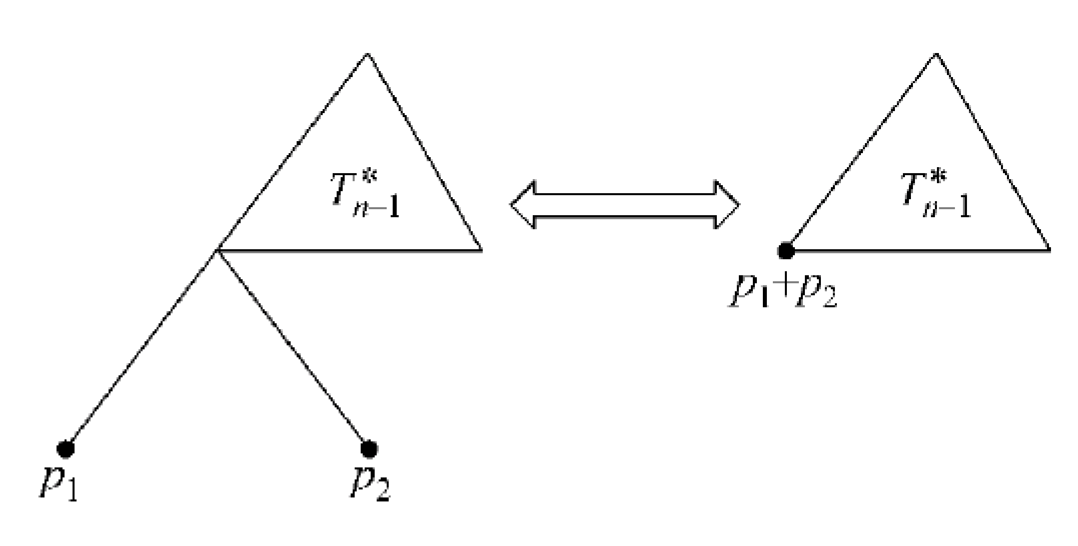


图 10-8　T_{n-1}^* 与 T_n^* 的关系

问题导致求 T_{n-1}^* 的最佳二分树，而且 $m(T_n^*)=m(T_{n-1}^*)+p_1+p_2$。

T_{n-1}^* 与 T_n^* 的关系用图表示如图 10-8 所示。

T_{n-1}^* 也递归利用上面的方法。

例 10-14　若带权 0.01，0.03，0.03，0.03，0.05，0.05，0.2，0.6，求最优编码，如图 10-9 所示。

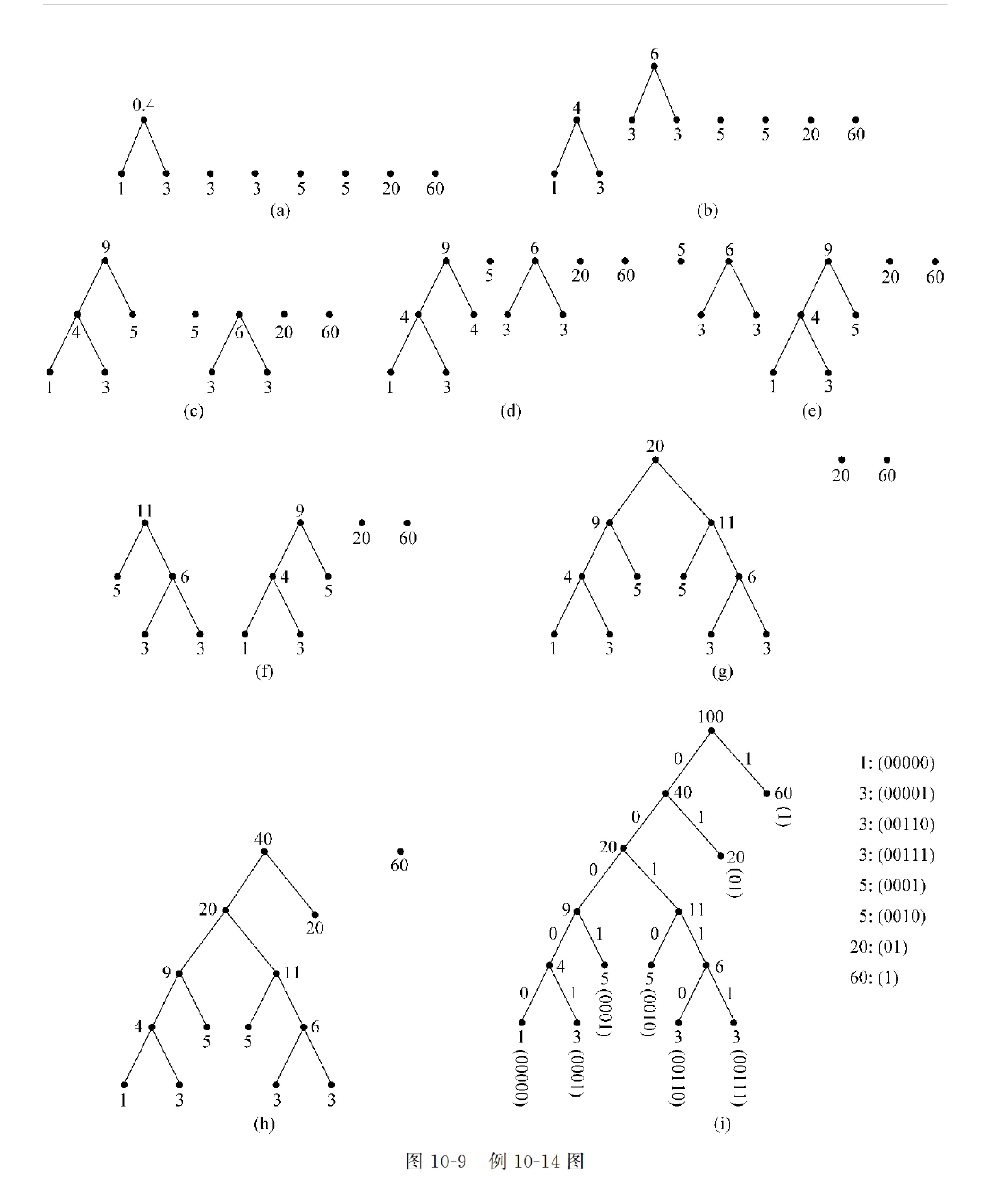


图 10-9　例 10-14 图

例 10-15　已知带权 0. 04，0. 06，0. 1，0. 14，0. 15，0. 16，0. 2，求最佳二元树，如图 10-10 所示。

4：(0000)

6：(0001)

10：(001)

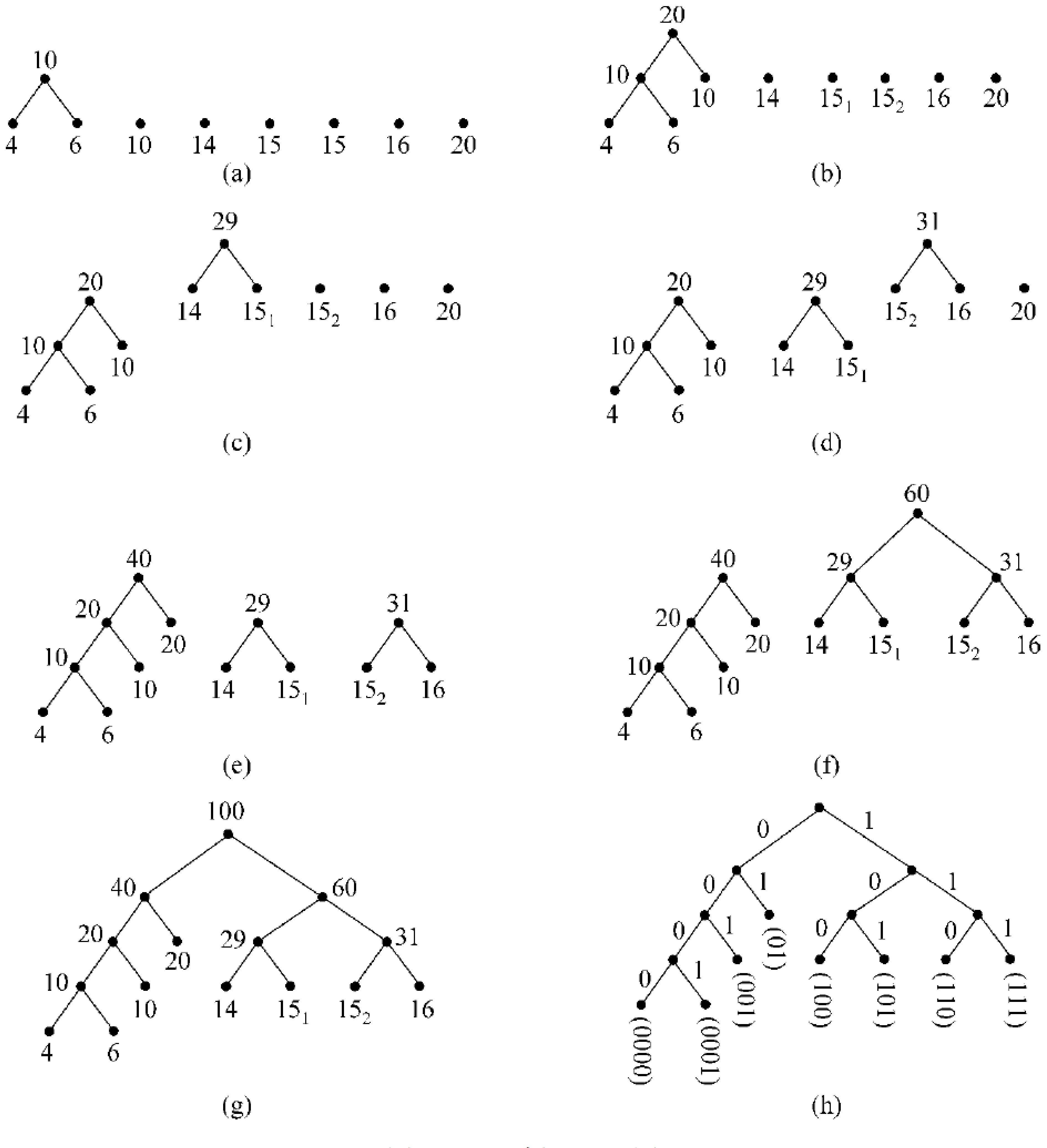


图 10-10 例 10-15 图

20：(01)

14：(100)

15_1：(101)

15_2：(110)

10：(111)

10.11 变长度码的译码方法

Huffman 树为最佳设计唯一可译码提供了有效的方法，它本身也是译码的不可或缺的工具，以 10.10 节例 10-13 若收到字符串 1110000001100111101 为例。

从树根，111 到了“树叶子”便得译码(10)，重新从树根开始 0000 又到“树叶”，又得译码(4)，重新从树根开始，001 再到“树叶”，译码(10)，101 译码(15_1)，如此等等。

10.12　分组码，Hamming 码

1. 基本概念

分组码与前面介绍的变长度码不同点在于它的码长都是一样的 0，1 符号串，其中比较实用的要推线性码，线性码的意思是：若 C_1 和 C_2 都是码字，都是长度为 n 的 0，1 符号串，$C_1 \oplus C_2$ 也是码字，$\oplus$ 是按位做异或运算的符号。

例如 $S=\{0100,0011,1100\}$，则 S 包含有

$0000\ 0100, 0100\oplus 0011=0111\ 0100\oplus 1100=1000$，

$0011\ 0011\oplus 1100=1111, 0100\oplus 0011\oplus 1100=1011$，

故 $S=\{0000,0100,0011,1100,0111,1011,1000,1111\}$。

定义 10-4：$V_1=(v_1^{(1)},v_2^{(1)},\cdots,v_n^{(1)})$，$V_2=(v_1^{(2)},v_2^{(2)},\cdots,v_n^{(2)})$ 是 n 维空间的两个向量。

$V_1 \cdot V_2 = v_1^{(1)}\cdot v_1^{(2)} \oplus v_2^{(1)}\cdot v_2^{(2)} \oplus\cdots\oplus v_n^{(1)}\cdot v_n^{(2)}$ 称为 V_1 和 V_2 的数量积，若 $V_1\cdot V_2=0$ 则称 V_1 和 V_2 正交。

例如在 $GF(2)$ 上两向量 $V_1=101011$，$V_2=011101$。

$V_1\cdot V_2=(0\cdot 1)\oplus(0\cdot 1)\oplus(1\cdot 1)\oplus(0\cdot 1)\oplus(1\cdot 0)\oplus(1\cdot 1)=1\oplus 1=0$。

故 V_1 和 V_2 正交。

已知 S 是一向量集合，V 是一向量，若所有属于 S 的向量都和 V 正交，则称 V 和 S 正交。和 S 正交的向量全体用 $S^{\perp}$ 表示，称为与 S 正交的空间。

例如 $S=\{0100,0101\}$，求 $(C_1C_2C_3C_4)$ 满足

$(0\cdot C_1)\oplus(1\cdot C_2)\oplus(0\cdot C_3)\oplus(0\cdot C_4)=1\cdot C_2$，

$(0\cdot C_1)\oplus(1\cdot C_2)\oplus(0\cdot C_3)\oplus(1\cdot C_4)=(1\cdot C_2)\oplus(1\cdot C_4)=C_2\oplus C_4$，

$C_2=0, C_4=0, C_1, C_3=0$ 或 1。

$S^{\perp}=\{0000,0010,1010,1000\}$，

生成矩阵与校验矩阵

$$\text{令 } \boldsymbol{G}=\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & g_{1,m+1} & g_{1,m+2} & \cdots & g_{1,n} \\ 0 & 1 & 0 & \cdots & 0 & g_{2,m+1} & g_{2,m+2} & \cdots & g_{2,n} \\ 0 & 0 & 1 & \cdots & 0 & g_{3,m+1} & g_{2,m+2} & \cdots & g_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & g_{m,m+1} & g_{m,m+2} & \cdots & g_{m,n} \end{bmatrix}_{m\times n}$$

对 $\boldsymbol{A}=(a_1a_2\cdots a_m)\in B^m$，对应有码字

$$\boldsymbol{W}=\boldsymbol{AG}=(a_1a_2\cdots a_m)\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & g_{1,m+1} & g_{1,m+2} & \cdots & g_{1,n} \\ 0 & 1 & 0 & \cdots & 0 & g_{2,m+1} & g_{2,m+2} & \cdots & g_{2,n} \\ 0 & 0 & 1 & \cdots & 0 & g_{3,m+1} & g_{2,m+2} & \cdots & g_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & g_{m,m+1} & g_{m,m+2} & \cdots & g_{m,n} \end{bmatrix}$$

$=(w_1 w_2 \cdots w_m w_{m+1} \cdots w_n)$,

$w_1=a_1, w_2=a_2, \cdots, w_m=a_m$,

$w_{m+j}=g_{1,j}w_1+g_{2,j}w_2+\cdots+g_{m,j}w_m, j=1,2,\cdots,n-m$。

这样的码字由两部分组成,一部分是信息位;另一部分是校验位,如图 10-11 所示。

例如 $\boldsymbol{G}=\begin{bmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{bmatrix}$,

$$(a_1a_2a_3)=\begin{bmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{bmatrix}=(a_1a_2a_3a_4a_5a_6)。$$

$a_4=a_1+a_3, a_5=a_1+a_2, a_6=a_2+a_3$

或写成

$$\begin{bmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}a_1\\a_2\\a_3\\a_4\\a_5\\a_6\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}$$

信息位		信息位	校验位
m位		m位	$n-m$位

图 10-11 码字

一般有

$$\begin{aligned}
&g_{1,m+1}w_1+g_{2,m+1}w_2+\cdots+g_{m,m+1}w_m+w_{m+1}=0\\
&g_{1,m+2}w_1+g_{2,m+2}w_2+\cdots+g_{m,m+2}w_m+w_{m+2}=0\\
&\vdots\\
&g_{1,m}w_1+g_{2,m}w_2+\cdots+g_{m,m}w_m+w_m=0
\end{aligned}$$

或写成矩阵形式

$\boldsymbol{H}\cdot\boldsymbol{W}=0$。

若 $\boldsymbol{G}=(\boldsymbol{I}_{(m)}\ \vdots\ \boldsymbol{A})_{m\times n}$ 则 $\boldsymbol{H}=(\boldsymbol{A}^{\mathrm{T}}\ \vdots\ \boldsymbol{I}_{(n-m)})_{(n-m)\times n}$。

$\boldsymbol{H}$ 称为校验矩阵,给定生成矩阵 $\boldsymbol{G}$,校验矩阵 $\boldsymbol{H}$ 便可得到;反之亦然,校验矩阵可用于纠正一个错误。

比如 $\boldsymbol{W}=(w_1w_2\cdots w_n)$ 在第 i 位传输错误,则

$\boldsymbol{HW}=e$,

$\boldsymbol{e}$ 将是 $\boldsymbol{H}$ 矩阵第 i 列向量,所以 $\boldsymbol{H}$ 矩阵必要满足:

(1) 无全零的列;

(2) 不存两列相等。

否则将出现一个错纠正不了,至出两位错误发现不了,$n-m$ 确定之后,n 最大不得超过 2^m-1。

$\boldsymbol{G}=(\boldsymbol{I}_{(m)}|\boldsymbol{A})_{m\times(2^n-1)}$,$\boldsymbol{H}=(\boldsymbol{A}^{\mathrm{T}}\ \vdots\ \boldsymbol{I}_{(2^n-m-1)})_{(2^n-m-1)\times n}$ 的码为 Hammig 码。

例 10-16 $n-m=3, n=2^3-1=7$

$$\boldsymbol{H}=\begin{bmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix},\quad \boldsymbol{G}=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}$$

$n-m=4, n=2^4-1=15$

$$\boldsymbol{H}=\begin{bmatrix}1&1&1&0&0&0&1&1&1&0&1&1&0&0&0\\1&0&0&1&1&0&1&1&0&1&1&0&1&0&0\\0&1&0&1&0&1&1&0&1&1&1&0&0&1&0\\0&0&1&0&1&1&0&1&1&1&1&0&0&0&1\end{bmatrix}$$

$$\boldsymbol{G}=\begin{bmatrix}1&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\0&1&0&0&0&0&0&0&0&0&0&1&0&1&0\\0&0&1&0&0&0&0&0&0&0&0&1&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&1&1&0\\0&0&0&0&1&0&0&0&0&0&0&0&1&0&1\\0&0&0&0&0&1&0&0&0&0&0&0&0&1&1\\0&0&0&0&0&0&1&0&0&0&0&1&1&1&0\\0&0&0&0&0&0&0&1&0&0&0&1&1&0&1\\0&0&0&0&0&0&0&0&1&0&0&1&0&1&1\\0&0&0&0&0&0&0&0&0&1&0&0&1&1&1\\0&0&0&0&0&0&0&0&0&0&1&1&1&1&1\end{bmatrix}$$

若信息量 $a=(10010111001)$ 它 Hamming 码 $a\boldsymbol{G}=\boldsymbol{R}$，

$\boldsymbol{R}=100101110010101$。

不难验证 $\boldsymbol{H}\boldsymbol{R}^{\mathrm{T}}=0$，即传输正确，予以接收，若到的是

$\boldsymbol{R}_1=1000^*01110010101$，

$\boldsymbol{H}\boldsymbol{R}_1^{\mathrm{T}}=(0110)^{\mathrm{T}}$ 可见传输出错，而 $(0110)^{\mathrm{T}}$ 是 $\boldsymbol{H}$ 矩阵的第 4 列，收第 4 位改 0 为 1，恢复了正确的传输，若收到

$\boldsymbol{R}_2=1000^*010^*10010101$，

$\boldsymbol{H}\boldsymbol{R}_2^{\mathrm{T}}=(1000)^{\mathrm{T}}$。

$(1000)^{\mathrm{T}}$ 是 $\boldsymbol{H}$ 的第 12 列，结果导致纠错了，Hamming 码只能纠一个错，出两位或两位以上的错比出一个错的概率小。

总之译码步骤如下，若收到的是 $\boldsymbol{R}=(r_1r_2\cdots r_n)$：

S1 计算 $\boldsymbol{S}=\boldsymbol{H}\boldsymbol{R}^{\mathrm{T}}$，$\boldsymbol{S}$ 称为纠正子。

S2 若 $\boldsymbol{S}=0$，则可认为传输正确，确原来信息 $m=r_1r_2\cdots r_m$，如若 $\boldsymbol{S}\neq 0$，则转 S3。

S3 若 $\boldsymbol{S}$ 是 $\boldsymbol{H}$ 的第 i 列，则认为 $\boldsymbol{R}$ 在第 i 位出错，予以纠正得 $\boldsymbol{R}_1$，取 $\boldsymbol{R}_1$ 的前 m 位为信息。

10.13　BCH 码

BCH 码是纠正多个错的编码，是由 Bose、Chandhuri 和 Hocquenghemm 同时发明的。下面仅就能纠两个错的 BCH(15,7) 码作为例子，介绍其编码和译码的过程，

BCH(15,7)指的是码长 15 位,信息 $m=m_0m_1\cdots m_6$ 共 7 位,生成多项式

$$g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)=x^8+x^7+x^6+x^4+1$$

其中 x^4+x+1 和 $x^4+x^3+x^2+x+1$ 都是在 $GF(2)$上为不可化约多项式编码方法之一,令

$$C(x)=x^8m(x)+r(x)=q(x)g(x)$$

其中 $q(x)$是 $x^8m(x)$除以 $g(x)$的商,$r(x)$为其余项,信息居于 $C(x)$的高位前面 7 位,可以验证如果 $\alpha\in GF(2^3)$并满足 $x^4+x+1=0$ 则 α^3 满足 $x^4+x^3+x^2+x+1=0$,所以码字多项式 $C(x)$满足 $C(\alpha)=0,C(\alpha^3)=0$。

令

$$\boldsymbol{H}(x)=\begin{bmatrix}1 & 2 & 3 & \cdots & 15\\ f(1) & f(2) & f(3) & \cdots & f(15)\end{bmatrix}=[\boldsymbol{h}_1 \quad \boldsymbol{h}_2 \quad \cdots \quad \boldsymbol{h}_{15}],$$

$$\boldsymbol{h}_i=\begin{pmatrix}i\\ f(i)\end{pmatrix},i=1,2,\cdots,15,$$

校下子 $\boldsymbol{S}=\boldsymbol{h}_i+\boldsymbol{h}_j=\begin{bmatrix}i+j\\ f(i)+f(j)\end{bmatrix}=\begin{pmatrix}s_1\\ s_2\end{pmatrix}$。

$$\begin{cases}i+j=s_1,\\ f(i)+f(j)=s_2,\end{cases}$$

若有适当的 $f(i)$可从此找到 i 和 j,比如 $f(i)=i^3$

$i+j=s_1,$

$i^3+j^3=s_2,$

$i^3+j^3=s_2=(i+j)(i^2+ij+j^2)=s_1(s_1^2+ij)=s_2,$

$ij=\frac{s_2}{s_1}+s_1^2,$

故 i,j 是下面二次方程的根:

$$x^2+s_1x+\left(\frac{s_2}{s_1}+s_1^2\right)=0。\quad (A)$$

(1) 若 $s_1=s_2=0$,无错误。

(2) 若 $s_1\neq 0,s_2=s_1^2$,有一个错误发生第 i 位。

(3) 若 $s_1\neq 0,s_2\neq s_1^2$,(A)式有两个根 i 和 j,则 $\boldsymbol{R}$ 在第 i 位和第 j 位有错误,予以纠正。

(4) 若(A)无解,或 $s_1=0,s_2\neq 0$,可能有超过两位错误发生,若 α 是 $GF(2^4)$的本原元素,$\alpha^{15}=1$

$$\boldsymbol{H}=\begin{bmatrix}1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14}\\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12}\end{bmatrix},$$

现在构造 $GF(2^4)$,设 $\alpha^4=1+\alpha,\alpha^5=\alpha+\alpha^2,\alpha^6=\alpha^2+\alpha^3,\alpha^7=\alpha^3+\alpha^4=1+\alpha+\alpha^3,$

$\alpha^8=\alpha+\alpha^2+\alpha^4=1+\alpha^2,\alpha^9=\alpha+\alpha^3,\alpha^{10}=\alpha^2+\alpha^4=1+\alpha+\alpha^2,\alpha^{11}=\alpha+\alpha^2+\alpha^3,$

$\alpha^{12}=\alpha^2+\alpha^3+\alpha^4=1+\alpha+\alpha^2+\alpha^3,\alpha^{13}=\alpha+\alpha^2+\alpha^3+\alpha^4=1+\alpha^2+\alpha^3,$

$\alpha^{14}=\alpha+\alpha^3+\alpha^4=1+\alpha^3,\alpha^{15}=\alpha+\alpha^4=1。$

$$H=\left[\begin{array}{ccccccccccccccc}
1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\
0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\
0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\
0&0&0&1&0&0&1&1&0&1&0&1&1&1&1\\
\hline
1&0&0&0&1&1&0&0&0&1&1&0&0&0&1\\
0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\
0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\
0&1&1&1&1&0&1&1&1&1&0&1&1&1&1
\end{array}\right],$$

矩阵上下各 4 行,依次为常数项,α,α^2,α^3,例如 $1+\alpha^2+\alpha^3$ 可以表示为

$$\begin{bmatrix}1\\0\\1\\1\end{bmatrix}$$

例校正子为

$s_1=1001,s_2=0101$,

$s_1=\alpha^{14},s_2=\alpha$,

$$\left[\frac{s_2}{s_1}\right]+s_1^2=\alpha^2+\alpha^{13}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}+\begin{bmatrix}1\\0\\1\\1\end{bmatrix}+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\alpha^{14},$$

$x^2+\alpha^{14}x+\alpha^{14}=(x+\alpha^8)(x+\alpha^6)$。

$$\alpha^6+\alpha^8=\begin{bmatrix}0\\0\\1\\1\end{bmatrix}+\begin{bmatrix}1\\0\\1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\alpha^{14},$$

故错发生在第 6 位和第 8 位。

这里运算都是在 $GF(2^4)$域上进行的。

习　　题

1. 一转轮分成 38 份,其中 2 绿,18 红,18 黑,向转轮掷上一小球,球停在 38 区域概率相等。

(1) 试问颜色的不确定性是多少?

(2) 颜色和数字的不确定性是多少?

(3) 若颜色已知,求 b 的条件熵。

2. 两口袋各有 20 个球,第一个口袋有 10 个白球,5 个红球,5 个黑球,第二个口袋有 8 个白球,8 个黑球,4 个红球,若从两口袋各取一球,试判定哪一口袋不确定较大。

3. 设有同一规格的银币 25 个,其中 24 个是合格的,重量相同,另一个是伪币,比其

他较轻，试求在不同砝码的天平上至少多少次可找到伪币。

4. 已知校验矩阵 $\boldsymbol{H}=\begin{bmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\1&1&1&0&0&1\end{bmatrix}$，求所有的码字，问能否纠一个错？

5. 已知生成矩阵 $\boldsymbol{G}=\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}$，求相应的校验矩阵。

6. 已知校验矩阵 $\boldsymbol{H}=\begin{bmatrix}1&1&0&1&1&0&0\\1&0&1&1&0&1&0\\0&1&1&1&0&0&1\end{bmatrix}$，求相应的生成矩阵。

7. C 是一长为 n，距离为 3 的二元码，C' 是取 C 的反，即 0，1 互换所组成：

(1) C' 码的距离是多少？

(2) C 和 C' 的码字组成的码能检出几个错，能纠出几个错？

8. BCH 码，若已知 $\boldsymbol{S}=\begin{bmatrix}\boldsymbol{s}_1\\\boldsymbol{s}_2\end{bmatrix}$：

$$\boldsymbol{s}_1=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\quad \boldsymbol{s}_2=\begin{bmatrix}1\\1\\0\\1\end{bmatrix}$$

试求错误所在的位，若

$$\boldsymbol{s}_1=\begin{bmatrix}1\\1\\1\\0\end{bmatrix},\quad \boldsymbol{s}_2=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

又如何？

参 考 文 献

[1] J S Chahal. Topics in Numbert Theory. New York：Plenum Press，1988.

[2] A Menezes. Elliptic Curve Public Key Cryptosystems. Boston：Kluwer Academic Publishers，1933.

[3] Man Young Rhce. Cryptography and Secure Communications. McGraw-Hill Book Go. 1994.

[4] Derek，John Scott Robinson. A Course in the Theory of Groups. NewYork：Springer-Verlag，1982.

[5] Neal Koblitz. Introduction to Elliptic Curves and Modular Forms. NewYork：Springer-Verlag，1993.

[6] S Gill，Williamson. Combinatorics for Computer Science. NewYork：Computer Science Press，2002.

[7] Neal Koblity. A Course in Number Theory and Cryptography. NewYork：Springer-Verlag，1994.